NTTME

MN8100WAG

ユーザーズマニュアル

■著作権表示について

本製品には次の条件下のソフトウェアが含まれています。

● Copyright © 2000-2003 Intel Corporation All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
* Neither name of Intel Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTEL OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES （INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION） HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT （INCLUDING NEGLIGENCE OR OTHERWISE） ARISING IN ANYWAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

● Copyright © 1997 - 2002, Makoto Matsumoto and Takuji Nishimura, All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of its contributors may not be used to endorse or promote products derived from this software without specific prior written permission.

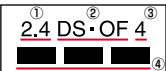
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

● Copyright © 2004 Atheros Communications,Inc., All Rights Reserved.

■商標についてのお知らせ

● Microsoft®、Windows®は、米国Microsoft® Corporationの登録商標です。
● Ethernet®は、富士ゼロックス社の登録商標です。
● Adobe® Acrobat® Reader™ 、Adobe® Readerは、アドビシステムズ社の商標です。
● AutoBACP™、AutoDNS™、AutoMP™、AutoNAT™、AutoPAD™、AutoPPP™、マルチアンサー™は、株式会社ビー・ユー・ジーの商標です。
● Super AG™は、Atheros Communications, Inc.の商標です。
● その他の商品名、会社名は、各社の商標または登録商標です。

■ご注意

【電波に関して】

● この装置は、情報処理装置等電波障害自主規制協議会（VCCI）基準に基づくクラスB情報技術装置です。この装置は家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近傍して使用されると受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。
● 本製品は電波法に基づき小電力データ通信システムの無線局の無線設備として、技術適合証明を受けています。したがって、本製品を使用するときに無線局の免許は必要ありません。
● 本製品は技術基準適合証明を受けていますので、以下の事項を行うと法律で罰せられることがあります。
 ・本製品を分解／改造すること
 ・本製品の裏面に貼ってある証明ラベルをはがすこと
● 本製品の使用周波数帯では、電子レンジ等の産業・科学・医療用機器等のほか工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）及び特定小電力無線局（免許を要しない無線局）が運用されています。
 1.本製品を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局が運用されていないことを確認して下さい。
 2.万一、本製品から移動体識別用の構内無線局に対して電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した上、下記連絡先へご連絡頂き、混信回避のための処置等（たとえば、パーテーションの設置など）についてご相談下さい。
 3.その他、本製品から移動体識別用の特定小電力無線局に対して電波干渉の事例が発生した場合など、何かお困りのことが起きましたら、下記連絡先へご連絡下さい。

連絡先：MNテクニカルセンタ
TEL　0570-055-128（NTT一般電話・携帯電話用）

【表示ラベルに関して】

● 本製品は、2.4GHz帯の周波数を使用する無線機器です。

本体に表示されている

は、以下の内容を意味します。
①使用している周波数帯域が2.4GHz帯であることを示します。
②変調方式がDS-SSおよびOFDM方式であることを示します。
③想定される干渉距離が40m以下であることを示します。
④全帯域を使用し、なおかつ移動体識別装置の帯域を回避可能であることを示します。

【その他】

● 本製品の故障、誤動作、不具合あるいは停電などの外的要因によって、通信などの機会を逃したために生じた損害などの純粋経済損失につきましては、当社は一切その責任を負いかねますので、あらかじめご了承下さい。
● 通信不良によって生じた損害につきましては、当社は一切その責任を負いかねますので、あらかじめご了承下さい。また、通信内容の漏れにつきましても、当社は一切その責任を負いかねますので、あらかじめご了承下さい。
● このマニュアルの著作権は、すべて株式会社 エヌ・ティ・ティ エムイーに帰属します。
● このマニュアルの内容の一部または全部を無断で転用することは禁止されています。
● このマニュアルおよびソフトウェア、ハードウェア、外観の内容について、将来予告なしに変更することがあります。
● このマニュアルで使用している「NTT」という用語は、「NTT東日本」「NTT西日本」または「NTTコミュニケーションズ」を指します。

安全にお使いいただくためにお読み下さい

本製品のご使用とお取り扱いに際して、次の点にご注意下さい。
ここでは、本製品を安全にお使いいただくために次のような絵表示を使って説明しています。

警告　この表示を無視して誤った取り扱いをすると、人が死亡又は重傷を負う可能性が想定される内容を示しています。

注意　この表示を無視して誤った取り扱いをすると、人が傷害を負う可能性が想定される内容および、物的損害のみの発生が想定される内容を示しています。

お願い　この表示を無視して誤った取り扱いをすると、本製品本来の性能を発揮できなかったり、機能停止を招く内容を示しています。

警告

◎お使いのとき（本体）

・煙が出ている、変なにおいがするなどの異常状態のまま使用すると、火災・感電の原因になります。ACアダプタを取り外し、煙が出なくなるのを確認してからMNテクニカルセンタへご連絡下さい。お客さまによる修理は大変危険ですから、絶対におやめ下さい。
・本製品を分解したり、改造したりしないで下さい。発熱・火災・感電・故障の原因になります。
・誤って本製品を落下させたり、強い衝撃を与えた場合、内部の部品が外れる可能性があります。本製品を振ってカタカタという音がしたとき、あるいは本製品の動作が不安定なときは、ACアダプタを取り外し、MNテクニカルセンタへご連絡下さい。そのまま使用すると、火災・故障の原因になります。
・本製品の内部に水などが入った場合は、ACアダプタを取り外し、MNテクニカルセンタへご連絡下さい。そのまま使用すると、火災・感電の原因になります。
・本製品が薬品や有害ガスに触れないようにして下さい。腐食する恐れがあります。また、本製品に有害な物質が付着することになり、人体に害をおよぼす恐れがあります。
・本製品の換気口をふさがないで下さい。発熱などにより、火災・感電・故障の原因になります。
・本製品の小さな穴を含むすべての穴に、異物を挿入しないで下さい。感電・故障の原因になります。万一異物が入ってしまった場合は、ACアダプタを取り外し、MNテクニカルセンタへご連絡下さい。そのまま使用すると、火災・感電・故障の原因になります。
・近くに雷が発生したときは、ACアダプタをコンセントから抜いて、すべてのケーブルを外し、ご使用をお控え下さい。ケーブルの接続や切断、又は製品の導入や保守の作業も行わないで下さい。雷によって、火災・感電の原因となることがあります。
・ケーブルを接続するときは、本製品および接続機器の電源を切ってから行って下さい。火災・感電・故障・事故の原因になります。

◎お使いのとき（ACアダプタ）

・ACアダプタは専用品以外を使用すると、発熱などで火災などの事故を起こす可能性があります。必ず本製品に添付のACアダプタをご使用下さい。また、本製品に添付されておりますACアダプタは本製品専用です。他の機器ではご使用にならないで下さい。
・ACアダプタを傷つけたり、破損したり、加工したり、コードを無理に曲げたり、引っ張ったり、ねじったり、きつく束ねたりしないで下さい。また重いものを載せたり、加熱したりするとACアダプタが破損し、火災・感電・故障の原因になります。ACアダプタが傷んだら、MNテクニカルセンタへご連絡下さい。

・ACアダプタはコンセントにしっかりと、最後まで差し込んで下さい。コンセントとの間に隙間があると、電極間にほこりやごみなどがたまり、漏電や火災の原因になります。時々電極間にほこりやごみがたまっていないかを確認して下さい。
・ぬれた手でACアダプタを抜き差ししないで下さい。感電・故障の原因になります。
・AC100Vの家庭用電源以外では、使用しないで下さい。火災・感電・故障の原因になります。
・ACアダプタを抜き差しするときは、必ずACアダプタ本体を持って行って下さい。ケーブルを直接引っ張るとケーブルが傷つき、火災・感電や断線の原因になります。

◎設置場所
・本製品のそばに花びん、植木鉢、コップ、化粧品、薬品の入った容器、又は小さな金属類を置かないで下さい。こぼれたり本製品の内部に入った場合、火災・感電の原因になります。
・直射日光のあたるところや、湿度の高いところに置かないで下さい。内部の温度が上がり、火災や故障の原因となることがあります。
・冷暖房機器の近くや、通風口からの風があたるところに置かないで下さい。火災や故障の原因となることがあります。
・ほこりの多い場所に置かないで下さい。火災・感電・故障の原因になります。
・調理台のそばなど油飛びや湯気の当たるような場所に置かないで下さい。火災・感電・故障の原因になります。

◎無線LANの電波に関して
・本製品は、医療機器、原子力設備や機器、航空宇宙機器、輸送設備など人命に関する設備や機器、および高度な信頼性を必要とする設備や機器としての使用、又はこれらに組み込んでの使用は意図されていませんので、使用しないで下さい。
・心臓ペースメーカをご使用の近くで、本製品をご使用にならないで下さい。心臓ペースメーカに電磁障害を及ぼし、生命の危険があります。
・医療機器の近くで、本製品をご使用にならないで下さい。医療機器に電磁障害を及ぼし、生命の危険があります。

⚠ 注意

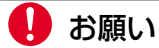
◎**お使いのとき**

・本製品に乗らないで下さい。特に小さなお子様のいる家庭ではご注意下さい。本製品が壊れて、けがの原因となることがあります。
・日本国以外で使用しないで下さい。本製品は、日本国内での使用を目的に設計・製造されています。したがって、日本国外で使用された場合、本製品およびその他の機器を壊す恐れがあります。また、当該国の法令に抵触する場合があるので、使用できません。
・本製品を5GHz帯で使用する場合は、電波法の定めにより屋外ではご使用になれません。
・本製品の改造および修理をしないで下さい。本製品は、法令に基づく承認を受けて製造されています。電気的・機械的特性を変更して使用することは、関係法令によって固く禁じられています。修理等はすべてMNテクニカルセンタにご依頼下さい。

◎**設置場所**

・極端な高温又は低温は、故障の原因になります。通常の室温（5〜35℃）でご使用下さい。
・結露するような場所で使用しないで下さい。温度差の激しい環境を急に移動した場合、本製品は結露する恐れがありますのでご注意下さい。故障の原因になります。結露した場合、本製品を乾燥させるか、長い時間同じ環境に置いた後、ご利用下さい。
・ぐらついた台の上や傾いたところなど、不安定な場所に置かないで下さい。また、本製品の上に重いものを置かないで下さい。バランスがくずれて倒れたり、落下してけがの原因となることがあります。
・動作中は内部の温度が上がり、本製品の外側も熱くなるため、他の装置等の上に本製品を重ねて設置しないで下さい。また、ビニール製のものなどを本製品のそばに置かないで下さい。変色・変形の原因になります。
・ガス腐食等を伴う環境（塩・酸・アルカリ等）には置かないで下さい。故障の原因になります。
・強い磁場を伴う環境には置かないで下さい。故障の原因になります。
・各ケーブルは所定のコネクタに接続して下さい。接続を誤ると、故障の原因になります。
・本製品やケーブルが人体などと接触するような場所に置かないで下さい。ケーブルの切断の原因や、落下による本製品の故障の原因になります。
・高圧線や通信用アンテナのそばでは、正しく通信できないことがあります。

◎無線LANの電波に関して

・電子レンジの近くで本製品を使用しないで下さい。電子レンジによって本製品の無線通信への電磁妨害が発生します。

お願い

◎お使いのとき
・動作中に接続ケーブルなどがはずれたり、接続が不安定になると、誤動作の原因になります。コネクタをしっかり接続し、動作中は、コネクタの接続部に触れないで下さい。
・本製品のそばにコードレス電話機やテレビなどの電子機器類を設置しないで下さい。電子機器類に雑音やノイズが発生したり、正常に動作しないことがあります。

無線LAN製品をご使用のとき【セキュリティ対策について】

※お客さまの権利（プライバシー保護）に関する重要な事項です。
無線LANでは、LANケーブルを使用する代わりに、電波を利用してパソコン等と無線アクセスポイント間で情報のやり取りを行うため、電波の届く範囲であれば自由にLAN接続が可能であるという利点があります。
その反面、電波はある範囲内であれば障害物（壁等）を越えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、次のような問題が発生する可能性があります。

●通信内容を盗み見られる
悪意ある第三者が電波を故意に傍受し、IDやパスワード、又はクレジットカード番号等の個人情報を盗み見られる可能性があります。

●不正に侵入される
悪意ある第三者が無断で個人や会社内のネットワークへアクセスし、個人情報や機密情報を取り出す（情報漏洩）、特定の人物になりすまして通信し不正な情報を流す（なりすまし）、傍受した通信内容を書き換えて発信する（改ざん）、コンピュータウィルスなどを流しデータやシステムを破壊する（破壊）、などの行為をされてしまう可能性があります。

本来、無線LANカードや無線アクセスポイントは、これらの問題に対応するためのセキュリティ機能を備えていますので、セキュリティに関する設定を行って製品を使用することで、その問題が発生する可能性は少なくなります。
なお、無線LANの仕様上、特殊な方法によりセキュリティ設定が破られることもあり得ますので、ご理解の上ご使用下さい。セキュリティの設定などについて、お客さま自身で対処できない場合にはMNテクニカルセンタまでご連絡下さい。
当社では、お客さまがセキュリティの設定を行わないで使用した場合の問題を十分理解した上で、お客さま自身の判断と責任においてセキュリティに関する設定を行い、本製品を使用することをお勧めします。

プロバイダを解約した場合のご注意

プロバイダ契約を解約したときは、そのプロバイダに接続するための設定を、本製品およびパソコンからすべて削除して下さい。削除しないまま本製品をお使いになると、意図しない接続料金を請求されることがあります。このような場合に生じた経済損失につきましては、当社は一切その責任を負いかねますのであらかじめご了承下さい。

本製品のマニュアルの使い方

使用しているマークについて

このマニュアルで、使用している記号の意味は次のとおりです。

アイコン	説　明
(注意アイコン)	ご注意していただきたい項目です。必ず目を通すようにして下さい。
Advice	補足的な情報を記載しています。
MEMO	知っておくと便利な情報を記載しています。
操作	本製品の操作や、パソコンの操作手順を記載しています。
設定ページ	設定ページでの設定の手順を記載します。

マニュアルの表記について

このマニュアルでは、次の用語を使用しています。

本製品：　「MN8100WAG」を指します。

ブロードバンド：　ADSL、CATV、FTTH（光ファイバ）を利用した通信を指します。

LAN上のパソコン：　「本製品のLANポートに接続しているパソコン」および「本製品のLANポートにつないだハブに接続しているパソコン」のことを指します。

Windows XP：　Microsoft Windows XP Home Edition（日本語版）およびMicrosoft Windows XP Professional（日本語版）を指します。

Windows 2000：　Microsoft Windows 2000 Server（日本語版）およびMicrosoft Windows 2000 Professional（日本語版）を指します。

Windows Me：　Microsoft Windows Millennium Edition（日本語版）を指します。

もくじ

導入編

クイック設定編

詳細設定編

拡張機能編

保守編

付録

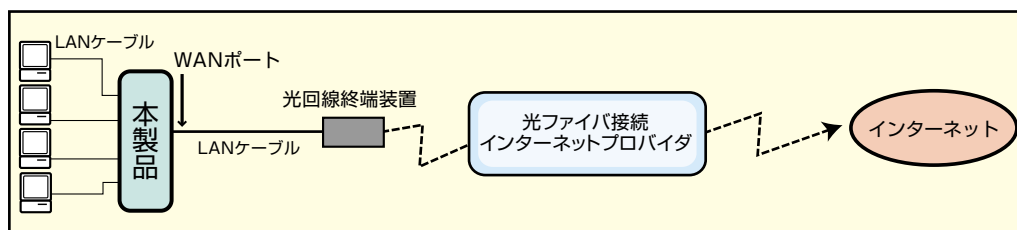
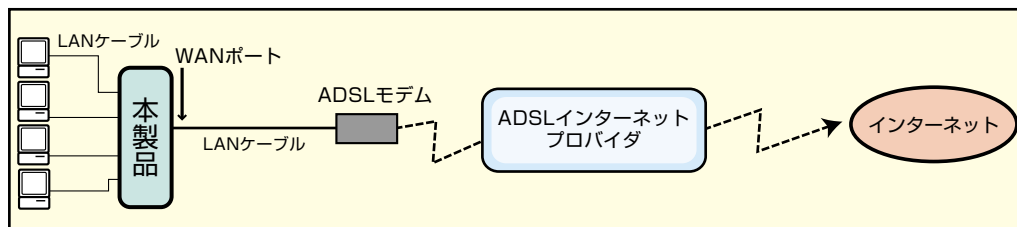
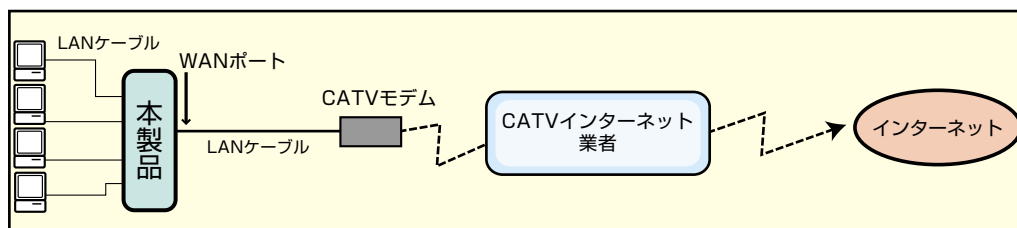
導入編

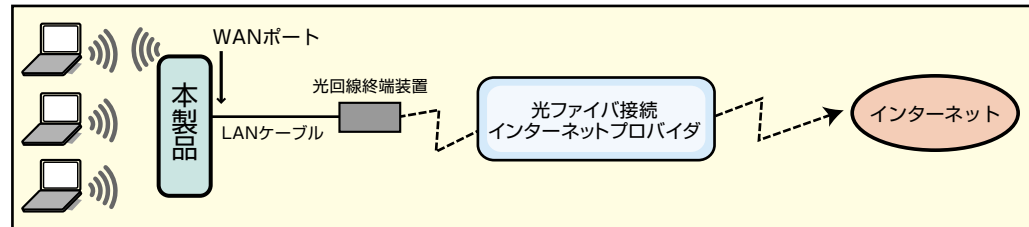
1 はじめに

製品概要

本製品は、ブロードバンド通信に対応したルータです。また、無線LANアクセスポイントを内蔵しているので、無線LANが構築できます。

■ブロードバンドでインターネット接続するときの形態例

Bフレッツなどの光ファイバでインターネット接続するとき

フレッツ・ADSLなどのADSLでインターネットに接続するとき

CATVインターネットに接続するとき

■無線LANを利用することもできます

無線LANを利用してBフレッツなどの光ファイバでインターネット接続するとき

■本製品の機能について

本製品の機能を、本書では次のように記載します。

ルータ機能	LANポート（LAN1～4）に接続したパソコンから、インターネットに接続する機能を指します。

■対応OS一覧

本製品は、下記OSに対応しています。
Microsoft Windows XP
Microsoft Windows 2000
Microsoft Windows Me

インターネットに接続するとき

高速スループット

ADSL、CATVインターネット、FTTHなど高速インターネットを快適に利用できます。

PPPoEクライアント/DHCPクライアント

PPPoEクライアント機能を搭載。PPPoEを採用しているプロバイダに接続してインターネットを利用できます。また、DHCPクライアント機能も搭載しているので、DHCP接続のプロバイダにも接続できます。

※ご契約の回線に応じて、回線に対応した光回線終端装置、ADSLモデム、CATVモデム等が必要です。

PPPoEマルチセッション

異なる複数のPPPoEセッションを最大4箇所まで同時に接続することができます。これによりプロバイダとフレッツ・スクウェア等、複数のプロバイダへの同時接続が可能となります。マルチセッション用の設定サンプルもあらかじめ用意されているので簡単です。

※ご契約の回線のPPPセッション数上限値が4セッションより少ない場合、回線の上限値が最大同時接続数となります。

PPPoEセッションキープアライブ

PPPoE接続が異常切断した場合でも、自動的に回線の接続を回復するセッションキープアライブ機能を搭載しています。

Unnumbered接続対応

複数のグローバルIPアドレスを取得してLAN型で接続する形態に対応しています。また、ネットワーク側にIPアドレスを付与しない、Unnumbered（アンナンバード）方式の接続形態にも対応しています。

VPNパススルー

PPTPパススルー、L2TPパススルー、IPSecパススルーの3種類のVPNパススルーに対応。企業内サーバ等へのセキュアなリモートアクセスが実現できます。

DMZホスト

インターネット側からのアクセスをLAN内の特定の端末に転送できるDMZ（DeMilitarized Zone）ホスト機能を搭載しています。NAT（Network Address Translation）またはNAPT（Network Address Port Translation）で変換されなかった通信をすべてDMZホストに転送することができます。使用ポートが特定できないネットワークゲームを使用する場合などに便利です。

※すべてのネットワークゲームに対応できるわけではありません。

UPnP

UPnP（Universal Plug and Play）に対応。Windows Messenger/MSN Messengerの音声チャットやファイル送信などが利用できます。
※LAN内の端末がUPnPに対応している必要があります。

ステートフル・パケット・インスペクション

受信したIPパケットの内容を読み取り、通過させるか破棄するかを自動的に判別する、ステートフル・パケット・インスペクションに対応。より強固なセキュリティが可能です。

ステルスモード

本製品はステルスモードを搭載していますので、インターネットからのPINGに応答しない、および、ICMPエラーを返さないことで外部にルータの存在を隠すことができ、ポートスキャンなどの攻撃から守ることができます。

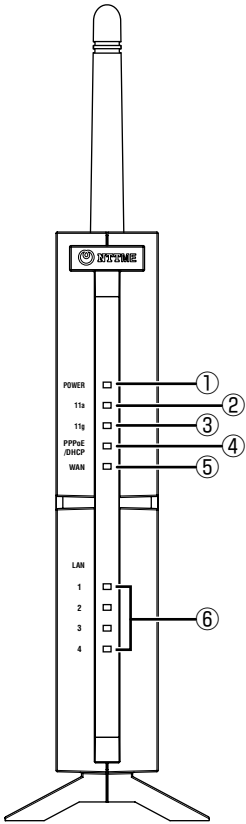
無線LAN機能

本製品で、無線LANを構築できます。IEEE802.11a、およびIEEE802.11g/bに対応。通信相手を特定するための識別番号SSIDに対応しているため、SSIDが一致した相手とのみ通信が可能です。また、本製品から発信するSSID情報を隠すこともできるので、不正アクセスの防止が可能です。WEP（Wired Equivalent Privacy）やWPA（WiFi Protected Access）をサポートしているため、無線LANのセキュリティ強度を大幅に向上させることができます。

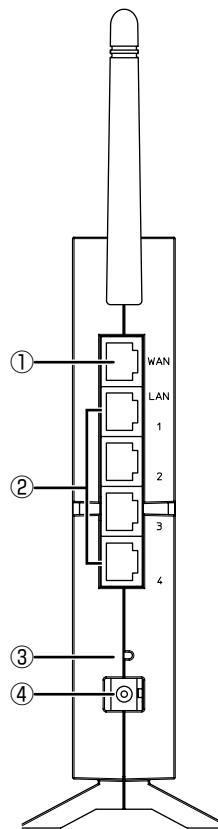
MACアドレスフィルタリング

無線で通信する際、登録したMACアドレスを持つ無線LAN端末以外からの接続を禁止することができます。

各部の名称とはたらき

■本体前面

名称	色	点灯時	点滅時
① POWER	緑	電源が投入されています。	
② 11a	緑		IEEE802.11a規格帯の無線LANが有効の状態です。
③ 11g	緑		IEEE802.11g/b規格帯の無線LANが有効の状態です。
④ PPPoE /DHCP	緑	PPPoE接続時にリンクが確立している状態です。または、DHCP接続時にIPアドレスを取得済みの状態です。 ※PPPoEのセッションごとにこのランプの点灯を制御することができます。 ☞「PPPoEオプション」〈P.55〉	PPPoE接続でリンク確立エラーの状態です。 ※消灯時は、PPPoE接続待機中、DHCP接続IPアドレス要求中、または固定IP接続中のいずれかの状態です。
⑤ WAN	緑	WANポートが使用可能な状態です。	WANポートでデータ転送中です。
⑥ LAN1～4	緑	LAN1～4ポートが使用可能な状態です。	LAN1～4ポートでデータ転送中です。

導入編

■本体背面

名称	説　明
① WANポート	LANケーブル※で、光回線終端装置/ADSLモデム/CATVモデムと接続します。
② LAN1～4ポート	LANケーブル※でパソコンを接続します。
③ RESETスイッチ	本製品の設定を購入時の状態に戻すときに押します。 ☞「RESETスイッチの動作について」〈P.182〉
④ DC INジャック	付属のACアダプタのプラグを差し込みます。

※:LANケーブルは本製品に1本のみ付属しています。WANポート、およびLAN1～4ポートのいずれかに使用できます。不足分はお買い求め下さい。

設置する前に確認して下さい

インターネットにアクセスするためには、次の準備が必要です。

■プロバイダと契約しましたか？

ADSLインターネットのプロバイダ、光ファイバ接続のプロバイダ、CATVインターネット業者のいずれかと契約する必要があります。

※ADSLインターネットのプロバイダと契約する場合は、DSL事業者との契約も必要なことがあります。詳しくは、プロバイダに確認して下さい。

※プロバイダによっては、接続する機器を事前に申請する必要があります。その場合、設定ページを開いて左側の［メンテナンス］の［WAN接続状況］→［DHCP/固定IP］をクリックして表示される画面のMACアドレス（「XX:XX:XX:XX:XX:XX」と表示されている番号）を申請します。☞「設定ページを開きます」〈P.28〉

※本製品のルータ機能では、1つのグローバルIPアドレスを複数のパソコンで使用してインターネットに接続します。プロバイダによっては、そのような接続を禁止している場合もあります。プロバイダとの契約内容を確認して下さい。

■工事は完了しましたか？

プロバイダの工事が完了してから、インターネットに接続することができます。

■必要な機器は用意しましたか？

次の機器が必要です。

光ファイバ接続のプロバイダと契約したとき：光回線終端装置
ADSLインターネットのプロバイダと契約したとき：ADSLモデム
CATVインターネットのプロバイダと契約したとき：CATVモデム
詳しくは、プロバイダにお問い合わせ下さい。

■ケーブルは揃っていますか？

LANケーブルは本製品に1本のみ付属しています。WANポート、およびLAN1～4ポートのいずれかに使用できます。不足分はお買い求め下さい。

■パソコンにLANポートはありますか？

本製品とパソコンを接続する場合、お使いのパソコンに、LANポートが必要です（10BASE-T、100BASE-TXのどちらも使用できます）。
お使いのパソコンにLANポートがない場合は、LANボードまたはLANカードをお買い求めの上、パソコンに取り付けて下さい。

■パソコンにインストールされているWWWブラウザを確認して下さい

●WWWブラウザのバージョンについて
本製品の設定には、WWWブラウザを使用します。下記のWWWブラウザがお使いのパソコンにインストールされているかどうか、確認して下さい。
・Microsoft Internet Explorer 6.0以上
・Netscape 7.1以上

●プロキシサーバ、JavaScriptの設定を確認する
・WWWブラウザでプロキシサーバを使用する設定になっていると、正しく操作できないことがあります。
※Windows版Microsoft Internet Explorer 6.0の場合
（1）［ツール］メニュー→［インターネットオプション］→［接続］タブをクリック
（2）［LANの設定］ボタンをクリック
（3）［ローカルエリアネットワークの設定］画面で［LANにプロキシサーバーを使用する］のチェックを外す
・WWWブラウザでJavaScriptを使用しない設定になっていると、正しく操作できません。

■別の機器につないだことのあるモデムを使う場合

ADSLモデムやCATVモデムによっては、最初につながれたネットワーク機器のMACアドレスを記憶し、それ以外のネットワーク機器とつなぐことを拒否する機種があります。このような場合は、一度ADSLモデムやCATVモデムの電源をOFFにして、10分程度経過してから、もう一度電源をONにして下さい。

※ADSLモデムやCATVモデムによっては、数時間から１日程度電源をOFFにすることが必要な機種もあります。
※プロバイダによっては、CATVモデムやADSLモデムの電源をOFFにすることを禁止している場合もあります。問題がないか確認してから、作業をして下さい。

2 パソコンの準備をしましょう

ネットワーク設定を行います

パソコンを本製品に接続した場合、出荷時の設定では、本製品からパソコンにIPアドレスが自動的に割り当てられます。このため、パソコン側では、「IPアドレスを自動的に取得」「DNSサーバのアドレスを自動的に取得」するように設定しておく必要があります。

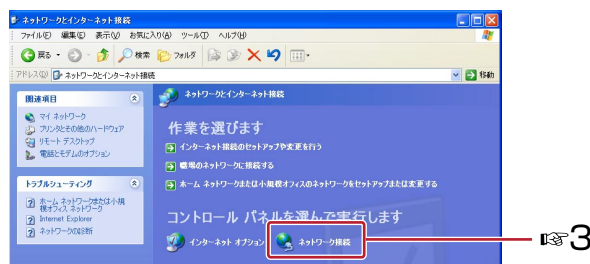
※本製品に接続するすべてのパソコンで、あらかじめネットワーク設定を行う必要があります。
※ネットワーク設定は、お使いのパソコンのOSごとに方法が異なります。ここではWindows XPの設定方法のみ解説します。その他のOSをお使いの方は、「Windows XP以外のOSでネットワークの設定をする」〈P.21〉を参照して下さい。

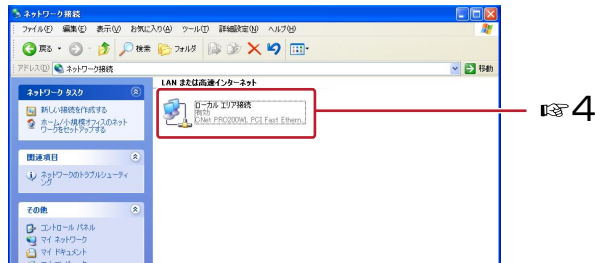
■Windows XPのネットワーク設定

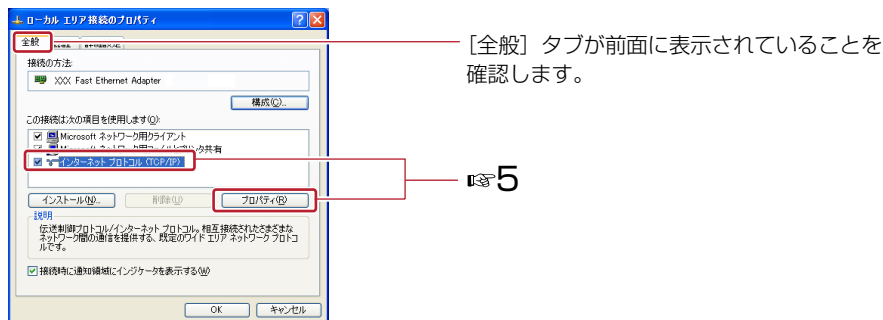
・ネットワークの設定を行うには、「コンピュータの管理者」または同等の権限を持つユーザでログオンする必要があります。
・以下の操作手順および画面表示は、Windows XPの初期状態の場合です。Windows XPの設定によっては異なる場合があります。

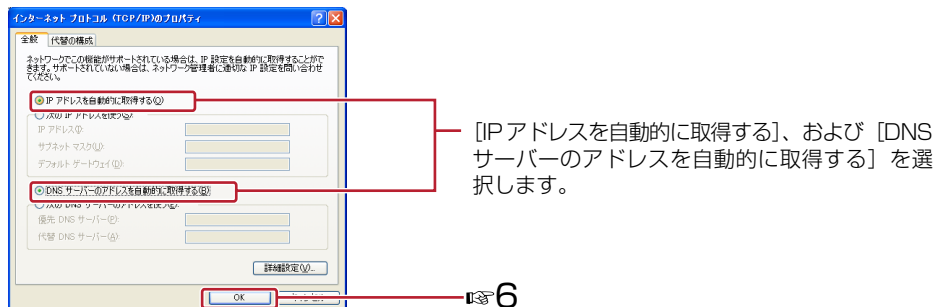
操作

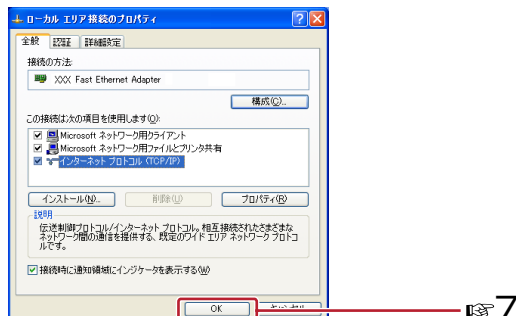
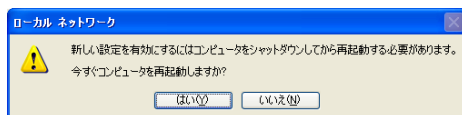
1 ［スタート］ー［コントロールパネル］を選択します。
 [コントロールパネル］ウィンドウが表示されます。

2 ［ネットワークとインターネット接続］をクリックします。
 ［ネットワークとインターネット接続］ウィンドウが表示されます。

3 ［ネットワーク接続］をクリックします。

［ネットワーク接続］ウィンドウが表示されます。

4 ［ローカルエリア接続］を右クリックし、表示されたメニューから［プロパティ］をクリックします。

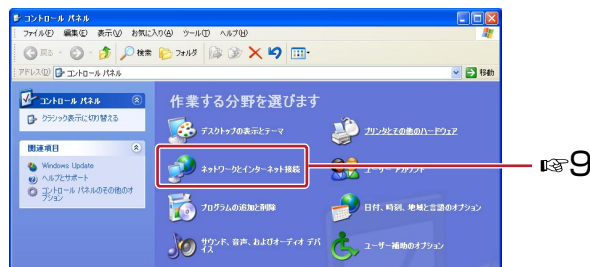
［ローカルエリア接続のプロパティ］ダイアログが表示されます。

5 ［インターネットプロトコル（TCP/IP)］を選択し、［プロパティ］ボタンをクリックします。

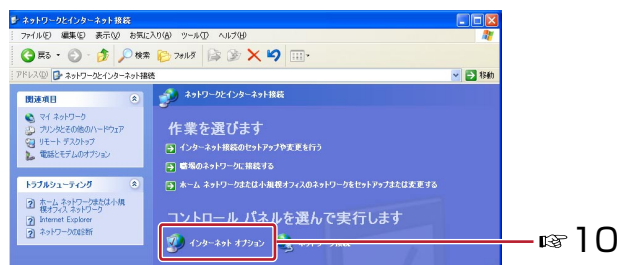
［インターネットプロトコル（TCP/IP）のプロパティ］ダイアログが表示されます。

6 ［OK］ボタンをクリックします。

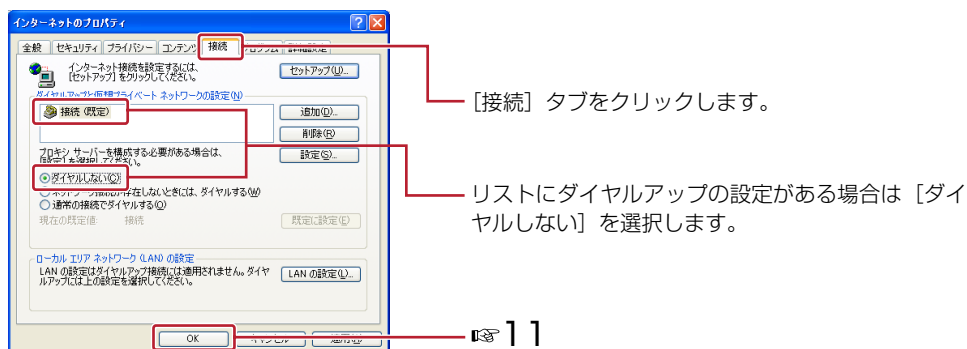
［ローカルエリア接続のプロパティ］ダイアログに戻ります。

7 ［OK］ボタンをクリックします。

再起動のメッセージが表示されたら、［はい］ボタンをクリックして、再起動して下さい。

8 ［スタート］－［コントロールパネル］を選択します。

［コントロールパネル］ウィンドウが表示されます。

9 ［ネットワークとインターネット接続］をクリックします。

［ネットワークとインターネット接続］ウィンドウが表示されます。

10［インターネットオプション］をクリックします。

［インターネットのプロパティ］ダイアログが表示されます。

11［OK］ボタンをクリックします。

以上で設定は終わりです。「本製品を設置しましょう」〈P.23〉へ進んで下さい。

◆Windows XP以外のOSでネットワークの設定をする

・Windows 2000の場合

※ネットワークの設定を行うには、「Administrator」または同等の権限を持つユーザでログオンする必要があります。

1 ［スタート］ー［設定］ー［コントロールパネル］を選択します。
［コントロールパネル］ウィンドウが表示されます。
2 ［ネットワークとダイヤルアップ接続］アイコンをダブルクリックします。
［ネットワークとダイヤルアップ接続］ウィンドウが表示されます。
3 ［ローカルエリア接続］アイコンをクリックします。
［ローカルエリア接続のプロパティ］ダイアログが表示されます。
4 ［インターネットプロトコル（TCP/IP）］を選択し、［プロパティ］ボタンをクリックします。
［インターネットプロトコル（TCP/IP）のプロパティ］ダイアログが表示されます。
5 ［IPアドレスを自動的に取得する］と［DNSサーバーのアドレスを自動的に取得する］を選択します。
6 ［OK］ボタンをクリックします。
［ローカルエリア接続のプロパティ］ダイアログに戻ります。
7 ［スタート］ー［設定］ー［コントロールパネル］を選択します。
8 ［インターネットオプション］アイコンをダブルクリックします。
［インターネットのプロパティ］ダイアログが表示されます。
9 ［接続］タブをクリックし、［ダイヤルアップの設定］のリストに設定が表示されている場合は、［ダイヤルしない］を選択します。
10 ［OK］ボタンをクリックします。

以上で設定は終了です。「本製品を設置しましょう」〈P.23〉へ進んで下さい。

・Windows Meの場合

1 ［スタート］ー［設定］ー［コントロールパネル］を選択します。
［コントロールパネル］ウィンドウが表示されます。
2 ［ネットワーク］アイコンをダブルクリックします。
※Windows Meで［ネットワーク］アイコンが表示されないときは、コントロールパネル左側の［すべてのコントロールパネルのオプションを表示する］をクリックして下さい。
［ネットワーク］ダイアログが表示されます。
3 リストの［TCP/IPー＞お使いのLANカード（またはLANボード）］を選択し、［プロパティ］ボタンをクリックします。
［TCP/IPのプロパティ］ダイアログが表示されます。
4 ［IPアドレス］タブをクリックし、［IPアドレスを自動的に取得］を選択します。
5 ［ゲートウェイ］タブをクリックします。
［ゲートウェイ］タブの設定画面に切り替わります。

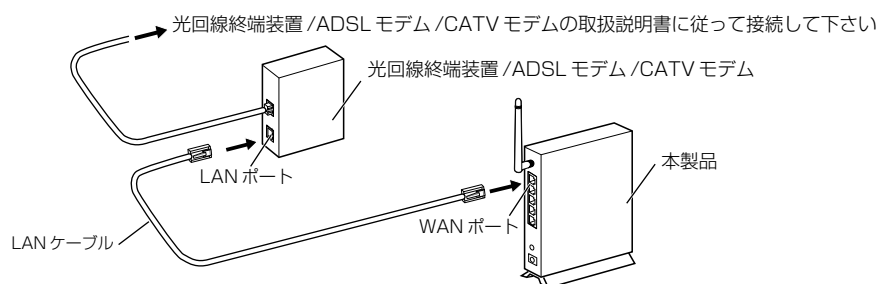
6 ［インストールされているゲートウェイ］に何もないことを確認します。
数字（IPアドレス）が表示されている場合は、表示されている数字を選択し、右の［削除］ボタンをクリックします。複数表示されている場合は、この操作を繰り返して、すべての内容を削除して下さい。
7 ［DNS設定］タブをクリックし、［DNSを使わない］を選択します。
8 ［OK］ボタンをクリックします。
［ネットワーク］ダイアログに戻ります。
9 ［OK］ボタンをクリックします。
再起動のメッセージが表示されたら、［はい］ボタンをクリックして、再起動して下さい。
10 再起動後、［スタート］－［設定］－［コントロールパネル］を選択します。
［コントロールパネル］ウィンドウが表示されます。
11 ［インターネットオプション］アイコンをダブルクリックします。
［インターネットのプロパティ］ダイアログが表示されます。
12 ［接続］タブをクリックします。
［ダイヤルアップの設定］リストにダイヤルアップの設定がある場合は、［ダイヤルしない］を選択します。
13 ［OK］ボタンをクリックします。

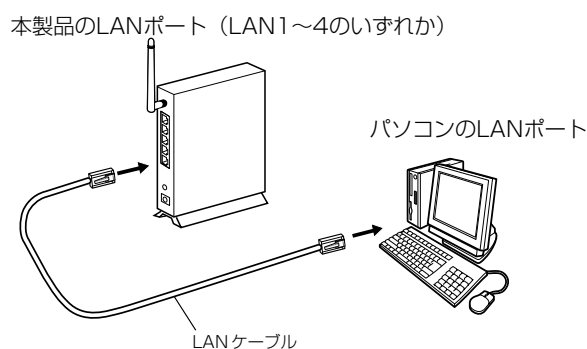
以上で設定は終了です。「本製品を設置しましょう」〈P.23〉へ進んで下さい。

3 本製品を設置しましょう

回線と本製品を接続しましょう

すべての機器の電源をOFFにしてから始めて下さい。本製品のACアダプタも接続しないで下さい。

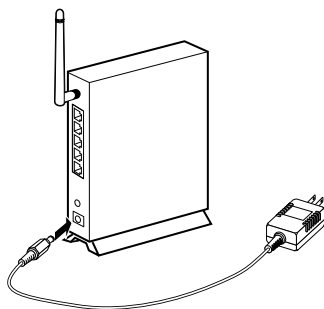
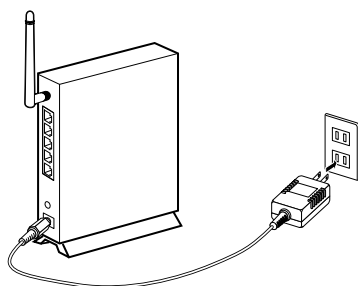
光回線終端装置/ADSLモデム/CATVモデムのLANポートと、本製品のWANポートを、LANケーブルで接続します。

本製品にパソコンを接続しましょう

パソコンの電源がOFFになっていることを確認して、本製品のLANポートと、パソコンのLANポートを、LANケーブルで接続します。

※本製品にハブを接続するときも、本製品のLANポートと、LANケーブルで接続して下さい。
※無線でパソコンを接続する場合は、「無線LAN設定」〈P.88〉を参照して通信できるようにして下さい。

ACアダプタを接続しましょう

操作

1　ACアダプタを接続する前に、モデムやパソコンが本製品とケーブルで正しく接続されているか、再確認して下さい。

2　付属のACアダプタのDC INジャックを本製品に差し込みます。

3　付属のACアダプタのプラグを家庭用電源コンセントに差し込みます。

正しく接続されている場合、本製品のランプは次のようになります。
POWER：点灯します。
WAN：光回線終端装置/ADSLモデム/CATVモデムに正しく接続されているときに点灯します。
LAN：パソコンのLANポートに正しく接続されているときに点灯し、データ転送中は点滅します。
11a/11g：点滅します。

クイック設定編

1 本製品の設定の流れ

ブロードバンドでインターネット

インターネット接続するためには、これから次の順番で設定を行います。

本製品にアクセスする

☞〈P.27〉

本製品に用意されている「設定ページ」にアクセスします。

ブロードバンドでインターネットに接続する

☞〈P.31〉

本製品に用意されている「設定ページ」で、ブロードバンド接続用のプロバイダの設定などを行います。

インターネットへの接続を確認する

☞〈P.43〉

「設定ページ」でプロバイダの設定を行った後に、有線LANもしくは無線LANで接続を確認します。

2 本製品にアクセスする

設定する前に確認して下さい

ブロードバンドでインターネットに接続する場合は、次の点を確認して下さい。

■プロバイダのタイプを確認して下さい

契約したプロバイダのタイプによって、操作手順が異なります。契約したプロバイダが次のどのタイプに該当するか、確認して下さい。

プロバイダのタイプ	説　明		プロバイダの例
PPPoEを使用しているプロバイダ(PPPoE接続)	PPPoEクライアントとも呼ばれます。IPアドレスはプロバイダから自動取得します。	「端末型」接続:プロバイダから割り当てられるIPアドレスが1つの場合	Bフレッツ/フレッツ･ADSL
		「LAN型」接続:プロバイダから複数のIPアドレスを割り当てられる場合	
PPPoEを採用していないプロバイダ(DHCP接続)	DHCPクライアントとも呼ばれます。IPアドレスはプロバイダから自動取得します。		Yahoo! BB/CATVなど
固定のIPアドレスを割り当てるプロバイダ	固定のIPアドレスをプロバイダから割り当ててもらいます。オプションのサービスとして提供されている場合もあります。		

※一般的な例で記載している内容は、変更になる場合があります。

■プロバイダから通知された情報を確認して下さい

①次の情報が必要です。お手元にご用意下さい。

- ログインユーザ名
- パスワード
- サービス名（プロバイダから通知された場合のみ）
- DNSサーバのIPアドレス（プロバイダから通知された場合のみ）

②PPPoEを採用していないプロバイダ（DHCP接続）の場合は、①に加えて以下の情報が通知されている場合があります。

- ゲートウェイアドレス

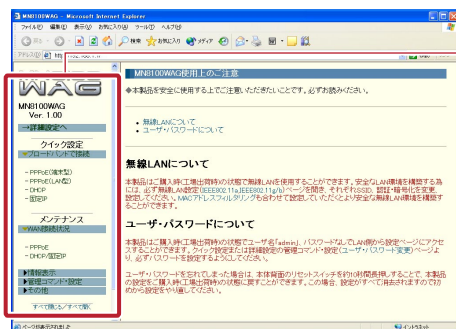
③IPアドレスを固定で割り当てるプロバイダの場合は、①に加えて以下の情報も必要です。

- IPアドレス
- サブネットマスク
- ゲートウェイアドレス
- DNSサーバのIPアドレス

設定ページを開きます

操作

1　WWWブラウザを起動します。

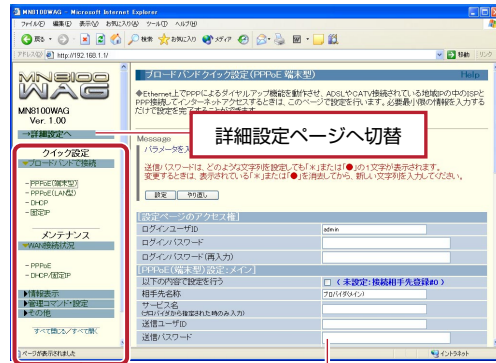
2　URLを入力する欄に「http://192.168.1.1/」と入力し、［Enter］キーを押します。
設定ページが表示されます。

画面左側に表示されるこの部分を
「メニュー」と呼びます。

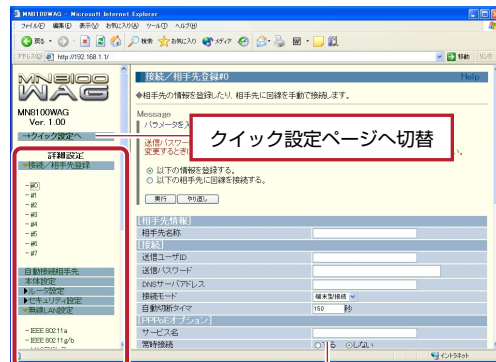
以降、この設定ページで本製品の設定を行います。なお、設定ページの設定は、1台のパソコンで行ってしまえば、ほかのパソコンで何度も行う必要はありません。

◆設定ページが開かないときは
設定ページが開かないときは、P.188を参照して下さい。

◆クイック設定ページと詳細設定ページについて

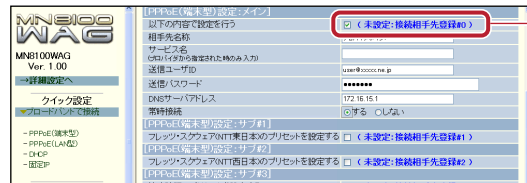
設定ページは、クイック設定ページと詳細設定ページの2種類から構成されています。この「クイック設定編」では、おもにクイック設定ページの使い方について解説しています。

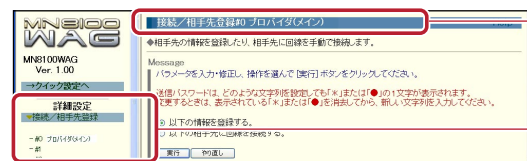
クイック設定ページ

クイック設定のメニュー　　クイック設定の画面

詳細設定ページ

詳細設定のメニュー　　詳細設定の画面

◆クイック設定ページで設定した内容が反映される接続相手先について

クイック設定ページとは、詳細設定ページで設定する内容のうち、必要最小限の項目が抜粋され、素早く設定ができるように設計された画面です。そのため、クイック設定ページで設定した内容は、詳細設定ページに反映されます。次の例で、設定が反映される様子を確認してみましょう。

※クイック設定ページで設定した一例

※クイック設定でインターネット接続の設定を行った場合、詳細設定の接続相手先登録の項目に反映されます。どの接続相手先に対して設定されるかは、この表示でわかります。
ここでは、接続相手先登録 #0 に対して設定を行っています。

上記の設定を行ったあと、詳細設定ページを開くと、次のように設定が反映されています。

接続相手先 #0 に、クイック設定で設定した内容が反映されていることがわかります。

接続相手先 #0 に、クイック設定で設定した内容が反映されています。

クイック設定ページと詳細設定の対応は次のとおりです（設定方法は次ページ以降で詳しく解説します）。

※クイック設定・詳細設定の対応表（<>内は本製品にあらかじめ用意されている設定です）

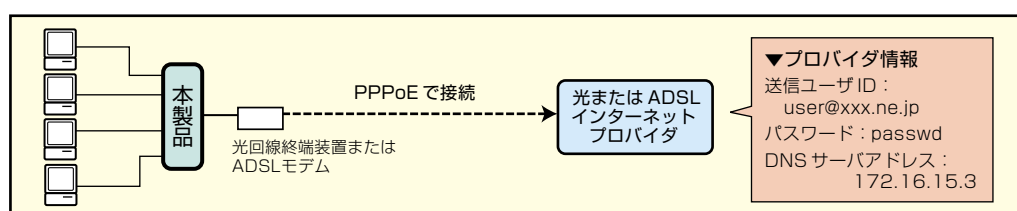
クイック設定ページ			詳細設定ページの接続相手先
ブロードバンド	PPPoE（端末型）	メイン	#0
		サブ#1 <フレッツ･スクウェア（NTT東日本）>	#1
		サブ#2 <フレッツ･スクウェア（NTT西日本）>	#2
		サブ#3 <速度確認>	#3
		サブ#4 <空白>	#4
		―	#5
		―	#6
		―	#7
	PPPoE（LAN型）	メイン	#0
		サブ#1 <フレッツ･スクウェア（NTT東日本）>	#1
		サブ#2 <フレッツ･スクウェア（NTT西日本）>	#2
		サブ#3 <速度確認>	#3
		サブ#4 <空白>	#4
		―	#5
		―	#6
		―	#7

3 ブロードバンドでインターネットに接続する

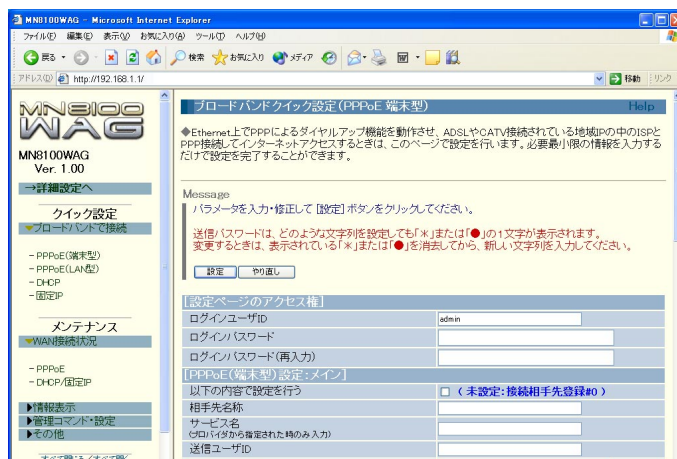
Bフレッツ、フレッツ・ADSLなど、PPPoEを採用しているプロバイダの場合

PPPoEを採用しているプロバイダに接続する場合、端末型とLAN型があります。それぞれ設定方法を解説します。該当する方をお読み下さい。

■PPPoEを採用しているプロバイダ（端末型）の場合

ここでは、次のような接続例を挙げて解説します。

設定ページ

1　メニューから［ブロードバンドで接続］をクリックし、［PPPoE（端末型）］をクリックします。

［ブロードバンドクイック設定（PPPoE端末型）］画面が表示されます。

2 ［PPPoE（端末型）設定：メイン］で、プロバイダに接続するための設定を行います。

ここで設定した内容は接続相手先 #0 に反映されることを示しています。また、「未設定」と表示されているので、接続相手先 #0 には何も設定が書き込まれていないことがわかります。

以下の内容で設定を行う	チェックします。（チェックしないと設定されないのでご注意下さい）
相手先名称	プロバイダ名など、任意の名称を入力します。
サービス名	プロバイダから指定されたときのみ入力します。（指定されていないときは空白）
送信ユーザID	プロバイダから指定されたユーザIDを入力します。「xxxxxx@xxxx.ne.jp」のようにすべて入力して下さい。また、半角英数字で入力して下さい。
送信パスワード	プロバイダから指定されたパスワードを入力します。半角英数字で入力して下さい。また、大文字･小文字を区別して入力して下さい。入力したパスワードはすべて「*」または「●」で表示されます。
DNSサーバアドレス	プロバイダから指定された場合、DNSサーバのIPアドレスを入力します。複数指定されている場合は、いずれか1つを入力して下さい。
常時接続	［する］［しない］のいずれかを選択します。

※［PPPoE（端末型）設定：サブ#1］～［PPPoE（端末型）設定：サブ#4］については、「PPPoEマルチセッションを利用する」〈P.45〉で解説します。

3　プロバイダの設定が終わったら、［設定］ボタンをクリックします。

「再起動後に設定が有効になります」という内容のメッセージが表示され、［再起動］画面が表示されます。

4　［再起動］ボタンをクリックします。

5　もとのページに戻ったあと、WWWブラウザを再起動します。

「インターネットへの接続を確認する」〈P.43〉に進んで下さい。

◆常時接続を［しない］に設定した場合

再起動後、WWWブラウザでURLを入力したり、メールソフトでメールの送受信を行ったりするまでは、インターネットには接続できません。

◆常時接続を［する］に設定した場合

再起動後、インターネットに自動的に接続します。一度インターネットに接続すると、切断しない限り接続されたままになります。プロバイダとの契約で、接続時間に応じて料金がかかる場合は、特にご注意下さい。

◆ほかの画面で設定するとき

［PPPoE（端末型）設定：メイン］は、詳細設定ページの接続相手先#0に反映され、自動接続先となります。このあと、別のクイック設定ページで設定を行うと、同じ接続相手先にその内容が反映され、先に行った設定が無効になることがあります。

☞「クイック設定・詳細設定の対応表」〈P.30〉

設定する際には、その項目で「未設定」と表示されているかどうか（「設定済」と表示されているときは、すでにその接続相手先には設定が行われています）をよく確認してから行って下さい。

◆［設定ページのアクセス権］について

本製品の設定ページへの不正なアクセスを防ぐために、クイック設定ページにある［設定ページのアクセス権］で管理者用のログインユーザID、ログインパスワードを設定することをお勧めします。

［設定ページのアクセス権］	
ログインユーザID	admin
ログインパスワード	••••••
ログインパスワード(再入力)	••••••

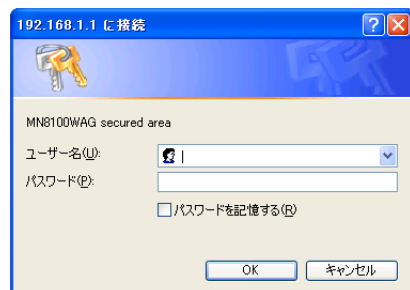
ユーザID/パスワードのメモ欄

ユーザID：

パスワード：

［設定ページのアクセス権］を設定した場合は、設定ページを開く際にログインユーザID、およびログインパスワードを入力する必要があります。設定したユーザIDとパスワードは忘れないようご注意下さい。万一忘れた場合は、本製品の設定を初期化する必要があります。

※初期化の方法は「RESETスイッチの動作について」〈P.182〉を参照して下さい。

◆［設定ページのアクセス権］の設定後について
ログインユーザIDとログインパスワードを設定した後、初めて［設定］ボタンをクリックしたときは、次のダイアログが表示されます。

［ユーザー名］［パスワード］欄に、設定したログインユーザID、ログインパスワードを入力して［OK］ボタンをクリックします。

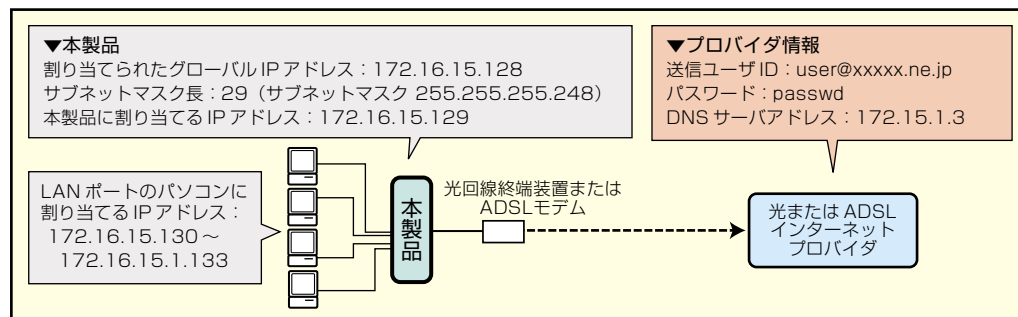
◆クイック設定の内容は、［詳細設定］画面にも反映されます

クイック設定	詳細設定
［設定ページのアクセス権］	［管理コマンド·設定］→［ユーザ·パスワード変更］
［PPPoE（端末型）設定:メイン］	［接続／相手先登録］→［#0］

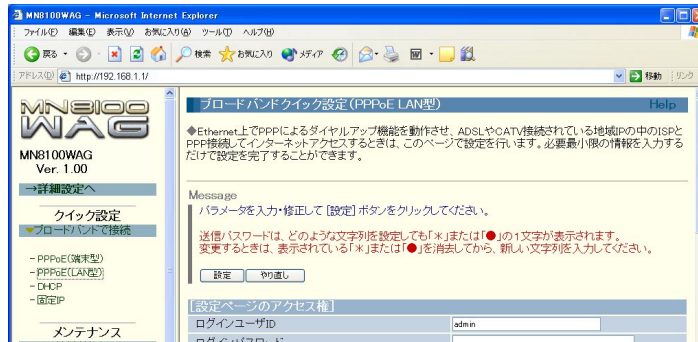
◆PPPoEセッションキープアライブ機能について
本製品には、PPPoEセッションキープアライブ機能があります。この機能により、プロバイダと接続中に、プロバイダ側から何らかの理由で切断された場合、自動で定期的に再接続を試みます。購入時は［有効］に設定されています。

◆自動的に設定されるフィルタについて
クイック設定を行うと、自動的にフィルタが設定されます。フィルタの内容については、「クイック設定で自動的に設定されるフィルタ」〈P.190〉を参照して下さい。

■PPPoEを採用しているプロバイダ（LAN型）の場合

ここでは、次のような接続例を挙げて解説します。

設定ページ

1　メニューから［ブロードバンドで接続］をクリックし、［PPPoE（LAN型）］をクリックします。

［ブロードバンドクイック設定（PPPoE LAN型）］画面が表示されます。

2　［LAN側設定］を設定します。プロバイダから割り当てられた連続したIPアドレスのうち、最初のアドレス（ネットワークアドレス）と最後のアドレス（ブロードキャストアドレス）はシステム側で使用されるため、通常は使用しません。P.34の例では、172.16.15.128～172.16.15.135の8個のIPアドレスのうち、172.16.15.128と172.16.15.135を除くアドレスを、本製品やLAN上のパソコン（ここでは4台）に割り当てます。

[LAN側設定]	
本体のIPアドレス/サブネットマスク長	172.16.15.129/29
DHCPサーバ機能	○OFF ◉ON
開始IPアドレス/個数	172.16.15.130/4
ドメイン名	

項目	説明
本体のIPアドレス/サブネットマスク長	本製品に設定するIPアドレスと、そのサブネットマスク長を入力します。
DHCPサーバ機能	本製品のDHCPサーバ機能を使うかどうか設定します。ここではDHCPサーバ機能を使うので［ON］に設定します。
開始IPアドレス/個数	LANポートに接続されたパソコンに割り当てる、開始IPアドレスと、割り当てる個数を「/」で区切って入力します。
ドメイン名	ドメイン名を使用する場合に入力します。

クイック設定編

3 ［PPPoE（LAN型）設定：メイン］で、プロバイダに接続するための設定を行います。

ここで設定した内容は接続相手先 #0 に反映されることを示しています。また、「未設定」と表示されているので、接続相手先 #0 には何も設定が書き込まれていないことがわかります。

以下の内容で設定を行う	チェックします。（チェックしないと設定されないので注意して下さい）
相手先名称	プロバイダ名など、任意の名称を入力します。
サービス名	プロバイダから指定されたときのみ入力します。（指定されていないときは空白）
送信ユーザID	プロバイダから指定されたユーザIDを入力します。「xxxxxx@xxxx.ne.jp」のようにすべて入力して下さい。また、半角英数字で入力して下さい。
送信パスワード	プロバイダから指定されたパスワードを入力します。半角英数字で入力して下さい。また、大文字･小文字を区別して入力して下さい。入力したパスワードはすべて「*」または「●」で表示されます。
DNSサーバアドレス	プロバイダから指定されたDNSサーバのIPアドレスを入力します。複数指定されている場合は、いずれか1つを入力して下さい。
常時接続	［する］［しない］のいずれかを選択します。

4 プロバイダの設定が終わったら、［設定］ボタンをクリックします。

「再起動後に設定が有効になります」という内容のメッセージが表示され、［再起動］画面が表示されます。

5 ［再起動］ボタンをクリックします。

6 もとのページに戻ったあと、WWWブラウザを再起動します。

「インターネットへの接続を確認する」〈P.43〉に進んで下さい。

クイック設定編

◆常時接続を［しない］に設定した場合
再起動後、WWWブラウザでURLを入力したり、メールソフトでメールの送受信を行ったりするまでは、インターネットには接続できません。

◆常時接続を［する］に設定した場合
再起動後、インターネットに自動的に接続します。一度インターネットに接続すると、切断しない限り接続されたままになります。プロバイダとの契約で、接続時間に応じて料金がかかる場合は、特にご注意下さい。

◆ほかの画面で設定するとき
［PPPoE（LAN型）設定：メイン］は、詳細設定ページの接続相手先#0に反映され、自動接続先となります。このあと、別のクイック設定ページで設定を行うと、同じ接続相手先にその内容が反映され、先に行った設定が無効になることがあります。
☞「クイック設定・詳細設定の対応表」〈P.30〉
設定する際には、その項目で「未設定」と表示されているかどうか（「設定済」と表示されているときは、すでにその接続相手先には設定が行われています）をよく確認してから行って下さい。

◆［設定ページのアクセス権］について
本製品の設定ページへの不正なアクセスを防ぐために、クイック設定ページにある［設定ページのアクセス権］で管理者用のログインユーザID、ログインパスワードを設定することをお勧めします。

［設定ページのアクセス権］を設定した場合は、設定ページを開く際にログインユーザID、およびログインパスワードを入力する必要があります。設定したユーザIDとパスワードは忘れないようご注意下さい。万一忘れた場合は、本製品の設定を初期化する必要があります。
※初期化の方法は「RESETスイッチの動作について」〈P.182〉を参照して下さい。

◆［設定ページのアクセス権］の設定後について
ログインユーザIDとログインパスワードを設定した後、初めて［設定］ボタンをクリックしたときは、次のダイアログが表示されます。

［ユーザー名］［パスワード］欄に、設定したログインユーザID、ログインパスワードを入力して［OK］ボタンをクリックします。

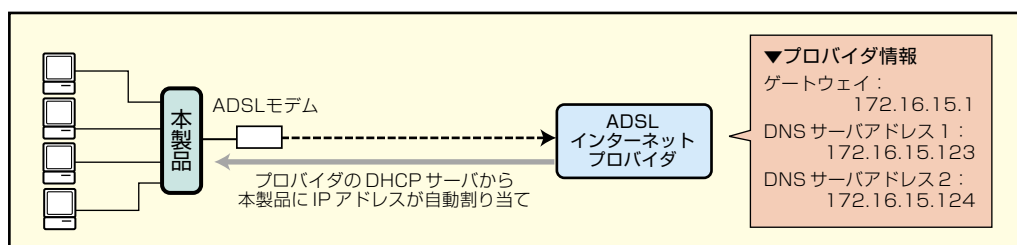
◆この画面で設定した内容は、［詳細設定］画面にも反映されます

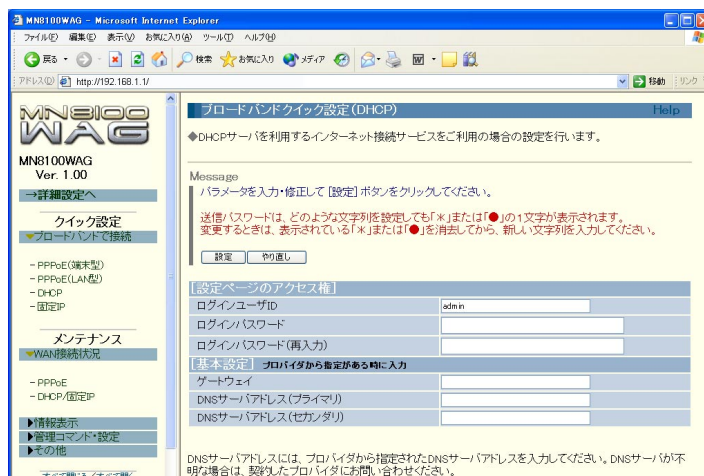
クイック設定	詳細設定
［設定ページのアクセス権］	［管理コマンド・設定］→［ユーザ・パスワード変更］
［LAN側設定］	［ルータ設定］→［LAN］
［PPPoE（LAN型）設定:メイン］	［接続／相手先登録］→［#0］

◆PPPoEセッションキープアライブ機能について
本製品には、PPPoEセッションキープアライブ機能があります。この機能により、プロバイダと接続中に、プロバイダ側から何らかの理由で切断された場合、自動で定期的に再接続を試みます。購入時は［有効］に設定されています。

◆自動的に設定されるフィルタについて
クイック設定を行うと、自動的にフィルタが設定されます。フィルタの内容については、「クイック設定で自動的に設定されるフィルタ」〈P.190〉を参照して下さい。

Yahoo! BBやCATVインターネットなど、PPPoEを採用していないプロバイダ（DHCP）の場合

ここでは、次のような接続例を挙げて解説します。

設定ページ

1　メニューから［ブロードバンドで接続］をクリックし、［DHCP］をクリックします。
［ブロードバンドクイック設定（DHCP）］画面が表示されます。

2 ［基本設定］で、プロバイダに接続するための設定を行います。プロバイダから指定がない場合は、空欄にしておきます。

［基本設定］ プロバイダから指定がある時に入力	
ゲートウェイ	172.16.15.1
DNSサーバアドレス（プライマリ）	172.16.15.123
DNSサーバアドレス（セカンダリ）	172.16.15.124

ゲートウェイ	プロバイダから指定された場合、ゲートウェイのIPアドレスを入力します。
DNSサーバアドレス（プライマリ/セカンダリ）	プロバイダから指定された場合、DNSサーバのIPアドレスを入力します。DNSサーバアドレスが1つしか指定されていない場合は、［DNSサーバアドレス（プライマリ）］のみ入力します。

3 プロバイダの設定が終わったら、［設定］ボタンをクリックします。

「再起動後に設定が有効になります」という内容のメッセージが表示され、［再起動］画面が表示されます。

4 ［再起動］ボタンをクリックします。

5 もとのページに戻ったあと、WWWブラウザを再起動します。

「インターネットへの接続を確認する」〈P.43〉に進んで下さい。

◆［設定ページのアクセス権］について

本製品の設定ページへの不正なアクセスを防ぐために、クイック設定ページにある［設定ページのアクセス権］で管理者用のログインユーザID、ログインパスワードを設定することをお勧めします。

［設定ページのアクセス権］を設定した場合は、設定ページを開く際にログインユーザID、およびログインパスワードを入力する必要があります。設定したユーザIDとパスワードは忘れないようご注意下さい。万一忘れた場合は、本製品の設定を初期化する必要があります。

※初期化の方法は「RESETスイッチの動作について」〈P.182〉を参照して下さい。

◆［設定ページのアクセス権］の設定後について
ログインユーザIDとログインパスワードを設定した後、初めて［設定］ボタンをクリックしたときは、次のダイアログが表示されます。

［ユーザー名］［パスワード］欄に、設定したログインユーザID、ログインパスワードを入力して［OK］ボタンをクリックします。

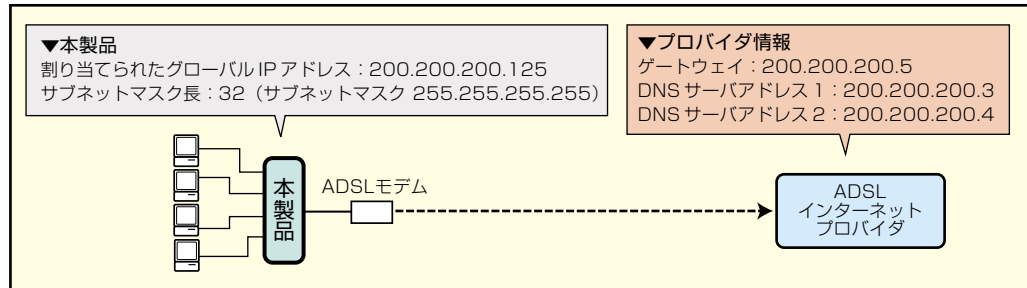
◆この画面で設定した内容は、［詳細設定］画面にも反映されます

クイック設定	詳細設定
［設定ページのアクセス権］	［管理コマンド･設定］→［ユーザ･パスワード変更］
［基本設定］	［ルータ設定］→［WAN］

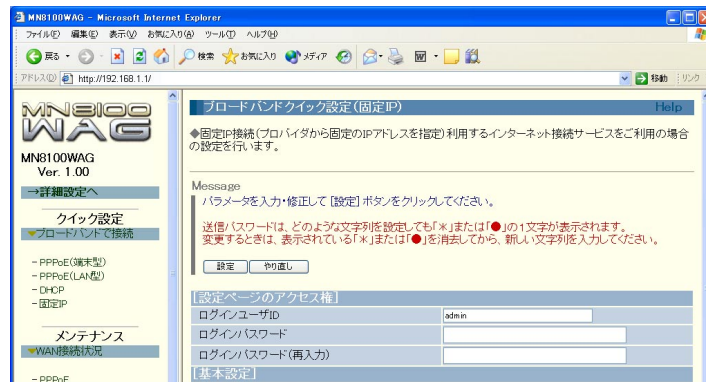
◆自動的に設定されるフィルタについて
クイック設定を行うと、自動的にフィルタが設定されます。フィルタの内容については、「クイック設定で自動的に設定されるフィルタ」〈P.190〉を参照して下さい。

すでにPPPoE（端末型）、またはPPPoE（LAN型）でご使用されていた場合には、プロバイダに関する情報をあらかじめ消去してから設定しなおして下さい。

固定のIPアドレスを割り当てるプロバイダの場合

ここでは、次のような接続例を挙げて解説します。

設定ページ

1 メニューから［ブロードバンドで接続］をクリックし、［固定IP］をクリックします。

［ブロードバンドクイック設定（固定IP）］画面が表示されます。

2 ［基本設定］で、プロバイダに接続するための設定を行います。

[基本設定]	
IPアドレス/サブネットマスク長	200.200.200.125/32
ゲートウェイ	200.200.200.5
DNSサーバアドレス(プライマリ)	200.200.200.3
DNSサーバアドレス(セカンダリ)	200.200.200.4

IPアドレス/サブネットマスク長	プロバイダから割り当てられた固定のグローバルIPアドレス、およびサブネットマスク長を入力します。
ゲートウェイ	ゲートウェイのIPアドレスを入力します。
DNSサーバアドレス（プライマリ/セカンダリ）	プロバイダから指定された場合、DNSサーバのIPアドレスを入力します。 DNSサーバアドレスが1つしか指定されていない場合は、［DNSサーバアドレス（プライマリ）］のみ入力します。

3 プロバイダの設定が終わったら、［設定］ボタンをクリックします。

「再起動後に設定が有効になります」という内容のメッセージが表示され、［再起動］画面が表示されます。

4 ［再起動］ボタンをクリックします。

5 もとのページに戻ったあと、WWWブラウザを再起動します。

「インターネットへの接続を確認する」〈P.43〉に進んで下さい。

◆［設定ページのアクセス権］について
本製品の設定ページへの不正なアクセスを防ぐために、クイック設定ページにある［設定ページのアクセス権］で管理者用のログインユーザID、ログインパスワードを設定することをお勧めします。

［設定ページのアクセス権］を設定した場合は、設定ページを開く際にログインユーザID、およびログインパスワードを入力する必要があります。設定したユーザIDとパスワードは忘れないようご注意下さい。万一忘れた場合は、本製品の設定を初期化する必要があります。
※初期化の方法は「RESETスイッチの動作について」〈P.182〉を参照して下さい。

◆［設定ページのアクセス権］の設定後について
ログインユーザIDとログインパスワードを設定した後、初めて［設定］ボタンをクリックしたときは、次のダイアログが表示されます。

［ユーザー名］［パスワード］欄に、設定したログインユーザID、ログインパスワードを入力して［OK］ボタンをクリックします。

◆この画面で設定した内容は、［詳細設定］画面にも反映されます

クイック設定	詳細設定
［設定ページのアクセス権］	［管理コマンド･設定］→［ユーザ･パスワード変更］
［基本設定］	［ルータ設定］→［WAN］

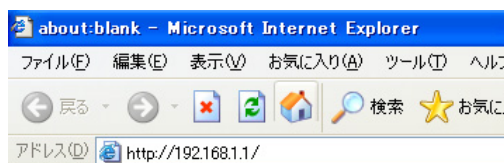
◆自動的に設定されるフィルタについて
クイック設定を行うと、自動的にフィルタが設定されます。フィルタの内容については、「クイック設定で自動的に設定されるフィルタ」〈P.190〉を参照して下さい。

LANケーブルを取り付けたパソコンからインターネット接続を確認する

インターネットに接続するための設定が終わったら、インターネットのWWWサイトにアクセスして下さい。WWWサイトが表示されたら、インターネットに接続されたことになります。WWWサイトが表示されなかった場合は、「WWWサイトが表示されなかった場合」を確認して下さい。

操作

1 WWWブラウザを起動します。

2 WWWブラウザのアドレスバーに「http://192.168.1.1/」を入力して、WWW設定画面にアクセスします。

3 ［メンテナンス］の［WAN接続状況］→［PPPoE］または［DHCP/固定IP］をクリックして、設定した接続またはセッションが「接続中」になっているか確認します。☞〈P.162〉

4 WWWブラウザのアドレスバーにWWWサイトのアドレス（例「http://www.ntt-me.co.jp/」）を入力します。
WWWサイトが表示されます。

これでインターネットに接続できるようになりました。ほかのLANポートに別のパソコンを接続して、同じようにWWWブラウザからインターネットに接続することを確認してみて下さい。

無線LANカードを取り付けたパソコンからインターネット接続を確認する

LANケーブルを取り付けたパソコンと同じ手順でWWWサイトにアクセスして下さい。WWWサイトが表示されなかった場合は、本製品および無線LANカードのSSID〈P.88、91〉、セキュリティ設定〈P.89、92〉が同一であるかを確認して下さい。同一であった場合は、次の「WWWサイトが表示されなかった場合」を確認して下さい。

クイック設定編

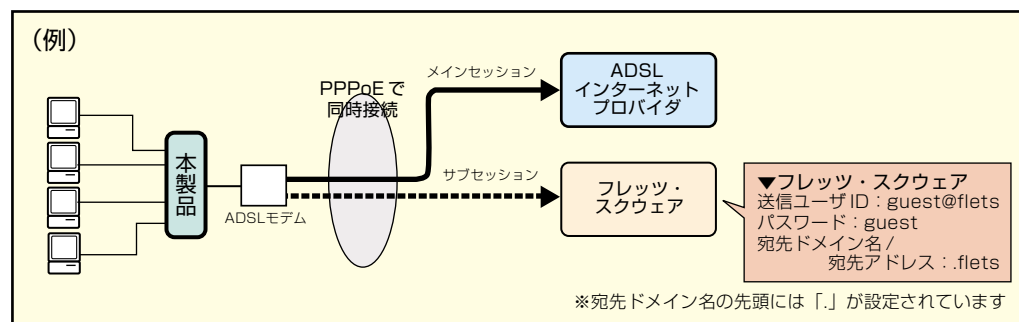
WWWサイトが表示されなかった場合

WWWサイトが表示されなかった場合は、次の項目を確認して下さい。詳細は、P.184を参照して下さい。

・パソコンを再起動して下さい。
・WWWサイトのアドレスがWWWブラウザのアドレスバーに正しく入力されているか、確認して下さい。
・「本製品にアクセスする」〈P.27〉を行ったか、確認して下さい。
・本製品とモデム等との接続を確認して下さい。
・パソコン、本製品、その他の機器の電源を適切な順番で入れたか、確認して下さい。詳細は、「本製品を設置しましょう」〈P.23〉を参照して下さい。
・プロバイダから受け取ったインターネットへの接続に関するアカウント情報を確認して下さい。設定値を入力する必要があれば、「ブロードバンドでインターネットに接続する」〈P.31〉を参照し、本製品に設定値を入力して下さい。
・PPPoE/DHCPランプが点灯していることを確認して下さい。

PPPoEマルチセッションを使用する方は「PPPoEマルチセッションを利用する」〈P.45〉へ進んで下さい。

5 PPPoEマルチセッションを利用する

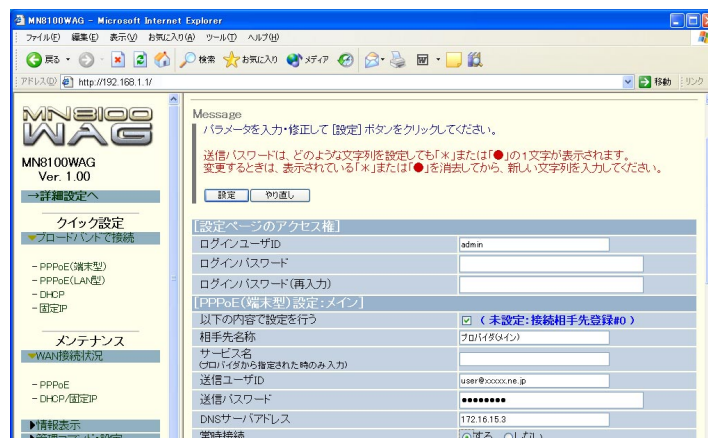
本製品では、PPPoEマルチセッション機能を使用することができます。この機能により、通常のインターネット接続をしたままフレッツ・スクウェアなどへ同時に接続を行うことができます。
本製品のPPPoEマルチセッションの設定を行うと、フレッツ・スクウェアなどのURLをWWWブラウザで指定するだけで、相手先に自動的に接続することができます。
ここでは、次のような接続例を挙げて解説します。（各設定項目の詳しい設定方法については、「サブセッションの設定項目について」〈P.49〉を参照して下さい）

プリセットされた［PPPoE（端末型）設定：サブ#1/サブ#2］では、初期値で自動切断タイマが［150］秒に設定されています。必要に応じて変更して下さい。☞〈P.55〉

フレッツ・スクウェアを利用する

通常接続するメインのプロバイダとしか契約していない場合でも、Bフレッツまたはフレッツ・ADSLユーザであれば、フレッツ・スクウェアに無料で接続できます。フレッツ・スクウェア用の設定を行い、接続してみましょう。

設定ページ

1 PPPoEマルチセッションを利用する場合は、メインセッションの設定を行います。設定ページのメニューから［ブロードバンドで接続］→［PPPoE（端末型）］または［PPPoE（LAN型）］をクリックします。

メインの設定欄に、通常接続するプロバイダを設定します。

2　フレッツ・スクウェアの設定を行います。

本製品の［PPPoE（端末型）設定：サブ#1/サブ#2］には、フレッツ・スクウェア（NTT東日本/NTT西日本）用の設定が用意されています。どちらか利用するサブセッションの［フレッツ・スクウェア（NTT東日本/NTT西日本）のプリセットを設定する］をチェックして下さい。

チェックします。（チェックしないと設定されないので注意して下さい）

3　［詳細設定］→［接続／相手先登録］→［#1（NTT東日本の場合）］または［#2（NTT西日本の場合）］で必要な設定を行います。

4　メインセッション、フレッツ・スクウェアのサブセッションの設定が終わったら、［設定］ボタンをクリックします。確認のダイアログが表示されたら、［はい］ボタンをクリックして下さい。

※お使いのWWWブラウザによっては、確認のダイアログが表示されないことがあります。

5　フレッツ・スクウェアに接続してみましょう。WWWブラウザのアドレス入力欄に、「http://www.flets/」と入力します。

［Enter］キーを押してフレッツ・スクウェアのホームページが表示されれば、サブセッションが確立しています（画面は一例です）。

速度測定サイトを利用する

NTT東日本エリアの東京、神奈川、千葉、埼玉エリアを除く地域で、各道府県ごとに設置された速度測定サーバを利用するには、あらかじめ用意されたサブセッション#3を使用します。

設定ページ

1 PPPoEマルチセッションを利用する場合は、メインセッションの設定を行います。設定ページのメニューから［ブロードバンドで接続］→［PPPoE（端末型）］または［PPPoE（LAN型）］をクリックします。

メインの設定欄に、通常接続するプロバイダを設定します。

2 速度測定サイトの設定を行います。

本製品の［PPPoE（端末型）設定：サブ#3］には、速度計測サイト用の設定が用意されています。［速度確認のプリセットを設定する］をチェックして下さい。

3 ［詳細設定］→［接続／相手先登録］→［#3］で必要な設定を行います。

4 設定が終わったら、［設定］ボタンをクリックします。確認のダイアログが表示されたら、［はい］ボタンをクリックして下さい。

※お使いのWWWブラウザによっては、確認のダイアログが表示されないことがあります。

5　速度測定サイトに接続してみましょう。すでにご契約の回線の最大セッション数を接続されている場合は、［メンテナンス］の［WAN接続状況］→［PPPoE］をクリックし、どちらかを切断して下さい。

WWWブラウザのアドレス入力欄に、「http://flets.speed/」と入力します。

［Enter］キーを押して速度測定のホームページが表示されれば、サブセッションが確立しています（画面は一例です）。契約しているフレッツサービスをクリックすると、速度を計測できます。

エリア内速度測定サイト

こちらのサイトにてお客様端末から地域IP網（エリア内のNTT区間）までの速度をご確認いただけます。

※ 表示される速度は測定中の速度の平均値であり、回線の最大速度を表すものではございません。また、結果として表示される速度は、ご利用の端末のOSや性能、及びその時のネットワークの混み具合やサーバへのアクセス状況等により変化致します。

● 「Bフレッツ　100Mbps」･･･「ビジネスタイプ」「ベーシックタイプ」「ニューファミリータイプ」「マンションタイプでPNAをご利用でない場合」のお客様はこちらにて測定してください。
● 「Bフレッツ　10Mbps」･･･「ファミリータイプ」「マンションタイプでPNAをご利用の場合」のお客様はこちらにて測定してください。

こちらのサイトにて、お客様端末からフレッツ網を経由して、エリア内のNTT区間まで※1の速度をご確認いただけます。

◆最大4箇所まで同時接続可能です

異なる複数のPPPoEセッションを、最大4箇所まで同時に接続することができます。ただし、ご契約の回線のPPPセッションの上限値が4箇所より少ない場合は、その上限値までの同時接続となります。

NTT東日本エリアでは、Bフレッツで2～4セッション、フレッツ・ADSLで2セッションが利用できます。NTT西日本エリアでは、Bフレッツで1～20セッション、フレッツ・ADSLで1～5セッションが利用できます。ただし、NTT西日本エリアの場合、利用するセッション数によって申込みまたはフレッツ・プラスの契約が必要になります。（平成15年9月現在）

詳細、最新情報については以下ホームページを参照して下さい。

NTT東日本　http://www.flets.com/

NTT西日本　http://www.ntt-west.co.jp/flets/

クイック設定編

◆サブセッションの設定項目について

接続する相手先に応じて、各項目を設定して下さい。サブの接続固有の設定項目は次のとおりです。

項目	説明
宛先ドメイン名/宛先アドレス	接続相手先のドメイン名、またはIPアドレスを指定します。インターネットに接続する際、ここで指定したドメイン名やIPアドレスで発信すると、この相手先へ接続されます。ただし、ドメイン名とIPアドレスを同時に指定することはできません。 ・カンマで区切って、4つまで設定できます。 ・IPアドレスの場合、ハイフンで区切ってアドレスの範囲を指定することもできます（xxx.xxx.xxx.xxx-yyy.yyy.yyy.yyy）。 ・空欄または＊ですべての宛先が対象となります。 （例）ホスト名の指定と、接続対象となる宛先 .jp：最後に.jpがつくサイトすべて .co.jp：最後に.co.jpがつくサイトすべて .www.ntt-me.co.jp：最後にwww.ntt-me.co.jpがつくサイトすべて （例:host.www.ntt-me.co.jp、host2.www.ntt-me.co.jpが該当しますが、www.ntt-me.co.jpは対象になりません） www.ntt-me.co.jpのみ："www.ntt-me.co.jp"のみ（先頭に「.」がついている場合との違いに注意して下さい） なお、本製品のAutoDNS機能をOFFにした場合、宛先ドメイン名を指定しても無効になります。
プロトコル	使用するプロトコルを限定したいときに1つだけ設定します。ニーモニック（esp、gre、icmp、ipencap、tcp、udp、tcp_udp）またはプロトコル番号で指定します。空欄または*ですべてのプロトコルが対象となります。
宛先ポート番号	TCP、UDPプロトコルで宛先ポート番号を限定したいときに設定します。ニーモニック、またはポート番号で指定します。空欄または*ですべてのポートが対象となります。
送信元アドレス	LAN上のパソコンのうち、その相手先に接続できるパソコンを限定したいときに設定します。 接続できるパソコンのIPアドレスを、次のように指定します。 ・xxx.xxx.xxx.xxxの形式で設定します。（例：192.168.1.3） ・ハイフンで区切ってアドレスの範囲を指定できます。 （例：192.168.1.3-192.168.1.5） ・末尾に/で区切ってサブネットマスク長を指定できます。 （例：192.168.1.0/29） ・空欄または＊ですべての宛先が対象となります。

※フレッツ・グループアクセスの設定方法については、P.144を参照して下さい。
※無線LANを構築したい方は、P.88を参照して下さい。

詳細設定編

1 はじめに

設定ページ

■設定ページについて

設定ページには、次の2種類があります。

クイック設定
本製品を使用するために最小限必要な設定をします(クイック設定編を参照して下さい)。

詳細設定
ルータ機能や無線LAN機能などの全機能を設定します。

設定ページで設定した内容は、本製品のフラッシュメモリに保存されます。
ACアダプタを取り外しても設定内容は失われません。

■設定ページの開き方

設定ページを開くときは、WWWブラウザのURLを入力する欄に、次の文字列を指定します。

http://［本製品のIPアドレス］/

購入時の本製品のIPアドレスは「192.168.1.1」です。本製品のIPアドレスを変更していないときは「http://192.168.1.1/」と指定できます。

2 接続／相手先登録

［接続／相手先登録］画面では、次の操作を行います。
・相手先の情報を登録する
・相手先に回線を接続する
相手先は、8件（登録番号#0～#7）まで登録できます。

「"」（ダブルクォーテーション）と半角スペースを続けて設定欄に入力することはできません。

●以下（以上）の情報を登録する。
設定した相手先の情報を登録するときに選択します。

●以下（以上）の相手先に回線を接続する。
相手先に接続するときに選択します。なお、登録していなくても、必須項目を入力するだけで相手先に接続できます。

●［実行］ボタン/［やり直し］ボタン
登録または接続するときは、［実行］ボタンをクリックします。
設定をやり直すときは、［やり直し］ボタンをクリックします。入力した内容が消去されます。
登録するときは［以下（以上）の情報を登録する。］、接続するときは［以下（以上）の相手先に回線を接続する。］をそれぞれ選択してから、［実行］ボタンをクリックします。

［実行］ボタンをクリックせずに他のページを開くと、入力した内容は消去されます。

■相手先情報

接続する相手先について設定します。

●相手先名称
相手先の名称を入力します（半角32文字、全角16文字以内）。
設定した名称は、詳細設定ページの画面左側に反映されます。通信には使用されませんので、わかりやすい名前を入力して下さい。

■接続

接続時に必要な情報について設定します。

●送信ユーザID

認証に必要なユーザIDを入力します。相手先（プロバイダなど）から指定されたユーザIDを入力します。

●送信パスワード

認証に必要なパスワードを入力します。どのような文字を入力しても、画面には「＊」や「●」の1文字が表示されます。

※次の文字および文字列は、使用できません。
「no」「clear」の文字列、「＊」「？」1文字のみ、漢字、ひらがな、カタカナ

●DNSサーバアドレス

相手先のDNSサーバのIPアドレスを入力します。
［ルータ設定（LAN）］画面の［AutoDNS機能］をONにしているときだけ使用できます。

◆［DNSサーバアドレス］を設定するとき

AutoDNS機能を使用すると、接続した際に相手先（プロバイダ）のDNSサーバのIPアドレスを自動的に取得できます。そのため、相手先のDNSサーバのIPアドレスを設定する必要はありません。
しかし、接続する相手先によっては、DNSサーバのIPアドレスを自動的に取得できないことがあります。接続後に正しく通信できない場合には、［DNSサーバアドレス］を設定して下さい。
DNSサーバのIPアドレスを取得できたかどうかは、設定ページのメニューから［WAN接続状況］→［PPPoE］をクリックし、［WAN接続状況（PPPoE）］画面で確認できます。

●接続モード

相手先とどのように接続するかを選択します。購入時は［端末型接続］に設定されています。

◆LAN型接続

ほかのLANやプロバイダにLAN型で接続します。

◆端末型接続

プロバイダに端末型で接続します。

●自動切断タイマ

タイマを設定して自動切断します。購入時は［150］秒に設定されています。
［クイック設定］→［PPPoE（端末型）］または［PPPoE（LAN型）］画面にある［PPPoE（端末型）設定：メイン］で設定した場合には、自動的に0秒（自動切断しない）が設定されます。

相手先に回線を接続中に一定時間以上通信がないときは、自動的に回線を切断することができます。

自動切断するまでの一定時間（10〜9999秒）を入力します。自動切断しないときは、「0」（ゼロ）と入力します。

※この項目は、常時接続の設定が［しない］に設定されたときのみ有効です。

ネットワークの設定内容や運用によっては、長時間、回線が接続したままになることや意図していない自動接続を行うことがあります。初期導入後は、必ず設定ページのメニューから［WAN接続状況］→［PPPoE］をクリックし、［WAN接続状況(PPPoE)］画面、あるいは本体前面のランプを確認して下さい。

特に次の環境で本製品を使用しないように注意して下さい。

・すでに稼動しているLANに本製品を導入する際、LANと同じサブネットのIPアドレスを本製品に設定しないまま、自動接続を行う設定にしているとき

・LAN上のパソコンで、定期的に回線を接続して通信を行うソフトウェアを起動しているとき

■PPPoEオプション

●サービス名

PPPoEを採用しているプロバイダに接続する際、プロバイダからサービス名（Service-Name）を指定された場合、そのサービス名を設定します。

●常時接続

登録した相手先に対して常時接続をするか設定します。

◆する

本製品の起動時に登録した相手先に自動的に接続し、接続中に何らかの理由で切断された場合、自動的に再接続します。ただし、手動で切断した場合は、再接続しません。

◆しない

PPPによるプロバイダとの接続を手動で行います。この場合、PPPの接続はメニューの上部もしくは下部にある［以下（以上）の相手先に回線を接続する。］にチェックをして、［実行］をクリックします。

●PPPoEランプ点灯

相手先接続時、PPPoEランプを点灯させるかどうか設定します。点灯する設定にした場合、認証失敗したときなどはPPPoEランプが点滅します。

◆する

PPPoEで通信中、本体前面のPPPoEランプが点灯します。

◆しない

PPPoEで通信中、本体前面のPPPoEランプは点灯しません。

◆接続時のPPPoEランプ点灯について
PPPoE通信時に、本製品前面のPPPoEランプが点灯するかしないかの違いで、通信方式自体には違いがありません。
クイック設定で設定すると、メインセッションは［する］が選択され、サブセッションの設定は［しない］が選択されます。

■マルチセッション選択ルール

1回線上でいくつかのPPPoE（PPP）接続を行うことで、複数の接続先を使い分ける機能のことを、「PPPoEマルチセッション」といいます。PPPoEマルチセッション機能を使うと、通常のインターネットに接続したまま、フレッツ・スクウェアなどへも接続することができます。
PPPoEマルチセッションを利用する場合は、［接続／相手先登録］の#0に、インターネットに接続するためのメインセッションの設定を行い、#1以降にサブセッションの設定をして下さい。
なお、クイック設定では、#1にフレッツ・スクウェア（NTT東日本）、#2にフレッツ・スクウェア（NTT西日本）の設定が用意されています。

●マルチセッション自動接続

◆する
マルチセッション自動接続を利用する。

◆しない
マルチセッション自動接続を利用しない。

●宛先ドメイン名/宛先アドレス
PPPoEマルチセッションの、専用アクセスポイントを設定するときに使用します。
接続相手先のドメイン名、またはIPアドレスを指定します。
ドメイン名の場合は、カンマで区切って4つまで設定できます。
IPアドレスの場合は1つ、またはハイフンで区切ってアドレス範囲を指定します。
※ドメイン名とIPアドレスを同時に指定することはできません。
※「xxx.xxx.xxx.xxx/mm」の形式でサブネットワークアドレスを指定することもできます。

●プロトコル
PPPoEマルチセッションの、専用アクセスポイントを設定するときに使用します。
使用するプロトコルを指定するときに、1つだけ設定します。
ニーモニック（esp、gre、icmp、ipencap、tcp、udp、tcp_udp）、またはプロトコル番号で指定します。

●宛先ポート番号
PPPoEマルチセッションの、専用アクセスポイントを設定するときに使用します。
宛先ポート番号を指定するときに設定します。
ニーモニック（ftp、ftpdata、telnet、smtp、www、pop3、sunrpc、nntp、ntp、login、pptp、domain、route）、またはポート番号で指定します。
何も入力しない場合は、すべてのポートが対象となります。

●送信元アドレス

PPPoEマルチセッションの、専用アクセスポイントを設定するときに使用します。LAN上の特定のパソコンのみこの接続を経由させたい場合、LAN上のパソコンのIPアドレスを指定します。

ハイフンで区切るとアドレスの範囲を指定できます。また、「xxx.xxx.xxx.xxx/mm」の形式でサブネットワークアドレスを指定することもできます。

■MTU設定

●MTUサイズ

PPPoEで通信時のMTU（Maximum Transmission Unit）の値を変更できます。

最大「1492」です。なお、Bフレッツ、フレッツADSLの場合は、自動的に「1454」となります。

■DoS攻撃防御設定

DoS攻撃とは、正式にはDenial of Service（サービス拒否）攻撃と言います。ネットワークを通じて不正なデータを送信したり、大量にデータを送信したりすることにより、相手のサービスを使用不能にする攻撃です。

DoS攻撃防御機能により不正なアクセスを検知し、本製品およびLAN側のネットワークを保護します。

●DoS攻撃防御

◆する

［セキュリティ設定］→［ルータ］で設定されたDoS攻撃防御を利用する。

◆しない

［セキュリティ設定］→［ルータ］で設定されたDoS攻撃防御を利用しない。

●ログ出力

DoS攻撃防御機能で破棄したパケットのログを出力できます。

◆する

ログを出力します。

破棄したパケットのログを出力するときは、［セキュリティ設定（ログ通知）］画面の［基本］で［NOTICE］をチェックして下さい。

◆しない

ログを出力しません。

◆プライベートアドレスのネットワークを接続する場合

DoS攻撃防御をオンにすると、IP Spoofing攻撃防御の機能がオンになり、送信元のIPアドレスがプライベートアドレスのパケットが破棄されます。そのため、以下のような通信ができなくなる場合があります。

・2拠点のプライベートアドレスネットワークをLAN型で接続する場合

・プライベートアドレスのLANにリモートアクセスする場合

この場合、該当する接続相手先のDoS攻撃防御の設定をオフにしてご利用下さい。

■オプション

相手先によっては、特別な設定が必要な場合があります。その場合はここで設定します。入力欄をクリックするとカーソルが表示されるので、コマンドを入力して下さい。コマンドを入力する際は、以下の点に注意して下さい。

・{ }で囲まれている部分がパラメータです。パラメータの区切りには、半角スペースを入力します。
・太字は、購入時の値を意味します。
・オプション以外のパラメータを省略すると、設定できません。
・複数のコマンドを設定するときは、コマンドごとに改行して下さい。
・文字列にスペースを含める場合は「"」で文字列を囲って下さい。(「ab cd」をコマンドとして入力する場合「"ab cd"」と入力して下さい)

●相手先自動接続の設定

自動接続をする設定の場合に、相手先ごとに自動接続するかどうかを指定します。ip routeの設定を変えず、一時的に自動接続の設定を変更したい場合などに利用します。

書式　**remote {rnumber} call auto {on｜off}**
パラメータ　{rnumber}=0〜7：相手先番号（登録番号#0〜#7）
{on｜off}
off：相手先への自動接続を行わない
on：相手先への自動接続を行う
設定例　ip route 0.0.0.0/32/7 remote 1 autoで、相手先#1へ自動接続の設定になっている場合でも相手先#1に自動接続したくないとき
→ remote 1 call auto off

●認証プロトコルの設定

接続する際の認証プロトコルを設定します。

書式　**remote {rnumber} call auth {none｜either｜pap｜chap}**
パラメータ　{rnumber}=0〜7：相手先番号（登録番号#0〜#7）
{none｜either｜pap｜chap}
none：PPP認証を行わない
either：相手先に合わせる
pap：PPP認証にPAPを使用する
chap：PPP認証にCHAPを使用する
設定例　相手先#2に接続する際、認証にPAPを使用するとき
→ remote 2 call auth pap

●IPアドレスネゴシエーションの設定

こちらからの最初の接続時にIPアドレスオプションのネゴシエーションを行なうかどうかを設定します（接続先から要求された場合は、ネゴシエーションを行います)。

書式　**remote {rnumber} ppp ipcp address {on｜off}**
パラメータ　{rnumber}=0〜7：相手先番号（登録番号#0〜#7）
{on｜off}
off：PPP（IPCP）でIPアドレスオプションのネゴシエーションを行わない
on：PPP（IPCP）でIPアドレスオプションのネゴシエーションを行う
設定例　相手先#1と接続する際、IPアドレスオプションのネゴシエーションを行わないとき
→ remote 1 ppp ipcp address off

●DNSサーバアドレスネゴシエーションの設定

接続時にDNSサーバアドレスのネゴシエーションを行なうかどうかを設定します。

書式　**remote {rnumber} ppp ipcp dns {on｜off}**

パラメータ　{rnumber}=0～7：相手先番号（登録番号#0～#7）

{on｜off}

off：PPP（IPCP）でDNSサーバアドレスのネゴシエーションを行わない

on：PPP（IPCP）でDNSサーバアドレスのネゴシエーションを行う

設定例　相手先#1と接続する際、DNSサーバアドレスのネゴシエーションを行わないとき

→remote 1 ppp ipcp dns off

●相手先ルータアドレスの設定

相手先ルータのIPアドレスを設定します。

書式　**remote {rnumber} rmtaddress {address}**

パラメータ　{rnumber}=0～7：相手先番号（登録番号#0～#7）

{address}：相手先ルータのIPアドレス

※ドットノーテーション（XXX.XXX.XXX.XXXの形式）で入力します。

設定例　相手先#1のルータのIPアドレス「192.168.5.100」を設定するとき

→remote 1 rmtaddress 192.168.5.100

●WAN側アドレスの設定

相手先との接続形態がLAN型で、WAN側で別のサブネットを使用するnumbered接続のとき、本製品のWAN側のIPアドレスを設定します。

書式　**remote {rnumber} wanaddress [{address}]/{mask}**

パラメータ　{rnumber}=0～7：相手先番号（登録番号#0～#7）

{address}：WAN側のIPアドレス

※ドットノーテーション（XXX.XXX.XXX.XXXの形式）で入力します。

{mask}：サブネットマスクまたはマスクビット数

※サブネットマスクは、ドットノーテーション（XXX.XXX.XXX.XXXの形式）で入力します。

設定例　相手先＃1とLAN型接続をする場合、WAN側にIPアドレス「192.168.1.1/24」を設定するとき

→remote 1 wanaddress 192.168.1.1/24

●PPPoEサーバ名の設定

PPPoEを採用しているプロバイダに接続する際、プロバイダからサーバ名（AC-Name）を指定された場合、そのサーバ名を設定します。

書式　**remote {rnumber} pppoe aname {name}**

パラメータ　{rnumber}=0～7：相手先番号（登録番号#0～#7）

{name}：PPPoEサーバ名

注意　このコマンドは、プロバイダから指定された場合のみ設定して下さい。

詳細設定編

●LCPエコーチェック機能の設定

LCPエコーチェック機能を使うと、PPPoEを採用しているプロバイダに接続中に、本製品側からプロバイダ側へ1分ごとにLCPエコー要求パケットを送信し、正しく接続しているかどうかをチェックします。プロバイダ側からの応答がない場合は、本製品側から切断します。購入時はLCPエコーチェック機能を使用する設定になっています。

書式　**remote {rnumber} pppoe echo {on｜off}**
パラメータ　{rnumber}=0〜7：相手先番号（登録番号#0〜#7）
{on｜off}
off：LCPエコーチェック機能を使用しない
on：LCPエコーチェック機能を使用する

●PPPoEセッションキープアライブ機能の設定

PPPoEセッションキープアライブ（Session Keep Alive）機能を使うと、PPPoEを採用しているプロバイダに接続中に、プロバイダ側から何らかの理由で切断された場合、自動的にプロバイダに再接続します。購入時はPPPoEセッションキープアライブ機能を使用する設定になっています。
なお、プロバイダに再接続している最中に、意図的に発信した場合や、自動接続した場合は、PPPoEセッションキープアライブ機能は停止します。また、PPPoEセッションキープアライブ機能による再接続は自動接続の対象にはなりません。ご注意下さい。

書式　**remote {rnumber} pppoe keepalive {on｜off}**
パラメータ　{rnumber}=0〜7：相手先番号（登録番号#0〜#7）
{on｜off}
off：PPPoEセッションキープアライブ機能を使用しない
on：PPPoEセッションキープアライブ機能を使用する

●PPPoEセッションキープアライブ拡張機能（常時接続）の設定

PPPoEセッションキープアライブ（Session Keep Alive）拡張機能を使うと、相手先がPPPoEを採用しているプロバイダの場合、本製品の起動時に自動的にプロバイダに接続し、接続中に何らかの理由で切断された場合、自動的にプロバイダに再接続します。また、プロバイダに再接続している最中に、意図的な発信や自動接続で接続に失敗した場合もPPPoEセッションキープアライブ拡張機能が動作します。
なお、PPPoEセッションキープアライブ拡張機能を使用すると、LCPエコーチェック機能の設定にかかわらず、自動的に［使用する］状態になります。PPPoEセッションキープアライブ拡張機能による再接続は自動接続制限の対象になりません。ご注意下さい。

書式　**remote {rnumber} pppoe always {on｜off}**
パラメータ　{rnumber}=0〜7：相手先番号（登録番号#0〜#7）
{on｜off}
off：PPPoEセッションキープアライブ拡張機能を使用しない
on：PPPoEセッションキープアライブ拡張機能を使用する

詳細設定編

3 自動接続相手先

● ［設定］ボタン
　設定を有効にするときは、［設定］ボタンをクリックします。

［設定］ボタンをクリックせずに他のページを開くと、設定した内容は消去されます。

■自動接続

［接続／相手先登録］画面に登録している相手先の中から、自動接続先を選択します。

●自動接続相手先
　自動接続先にする相手先を選択します。

●常時接続
　登録した相手先に対して常時接続をするか設定します。

◆する
　WAN側リンク確立時にPPPを自動接続します。また、何らかの理由でPPPが切断された場合も自動的に再接続します。

◆しない
　PPPによるプロバイダとの接続を手動で行います。

4 本体設定

● ［設定］ボタン/［やり直し］ボタン
　設定を有効にするときは、［設定］ボタンをクリックします。
　設定をやり直すときは、［やり直し］ボタンをクリックします。入力した内容が消去されます。

◆［設定］ボタンをクリックせずに他のページを開くと、設定した内容は消去されます。

◆「"」（ダブルクォーテーション）と半角スペースを続けて設定欄に入力することはできません。

■本体設定

●本体の名称
　本製品の名称を英数字で設定します。購入時は［MN8100WAG］に設定されています。
　設定した内容は、詳細設定ページの画面左側に反映されます。
　また、設定ページへアクセスするときに使用できます。詳しくは、「設定ページの開き方」〈P.52〉を参照して下さい。

●現在本体に設定されている日付と時刻
　日付と時刻を設定しても、ACアダプタを取り外した場合は、「1996/01/01-00:00」に初期化されます。
　初期化されたときは、［設定する日付と時刻］で再度正しい日付と時刻を設定して下さい。

●設定する日付と時刻
　「2003/01/01-00:00」のように、西暦（4桁）、月、日、時刻を入力します。西暦、月、日は「/」（スラッシュ）で、日付と時刻は「-」（ハイフン）で区切って下さい。
　設定した内容は、情報表示の各画面に反映されます。

◆本製品の日付と時刻の設定方法
本製品に日付と時刻を設定する方法には、手動設定と自動設定があります。

・手動設定

（1）［本体設定］画面の［設定する日付と時刻］で設定します。
（2）クイック設定ページで設定を行います。自動的に、設定を行ったパソコンの日付と時刻が設定されます。
（3）［本体設定］画面で「自動時刻修正」を使用する設定を行い、画面下の［今すぐ修正］ボタンを押します。

※（1）（3）の方法で設定した場合は、すでに日付と時刻が設定されているかどうかに関わらず、その設定内容に更新されます。

・自動設定

次のような場合に、自動的に日付と時刻が設定されます。

（1）ACアダプタを取り付けて本製品の電源をONにしたときに日付と時刻が設定されていない場合、本製品はLAN上に時刻を要求するパケットを送信します。LAN上にUnixマシンなどのタイムサーバ機能を持ったサーバが接続されている場合は、そのサーバから時刻を返答するパケットが送信されます。本製品はそのパケットを受信して、その内容を設定します。
複数のサーバから時刻を返答するパケットが送信された場合は、最初に受信したパケットの内容を設定します。
（2）上記（1）でパケットを受信できなかった場合は、本製品のルータ機能を使って回線を接続したときに、相手先のDNSサーバとNTPサーバに対して（LAN上のDNSサーバを指定している場合は、そのサーバが優先されます）時刻を要求するパケットを送信します。相手先のDNSサーバとNTPサーバから時刻を返答するパケットが送信されると、本製品はそのパケットを受信して、その内容を設定します。
ただし、本製品同士を接続した場合、自動設定は行われないことがあります。
（3）［本体設定］画面で「自動時刻修正」を使用する設定を行います。

■時刻修正機能

時刻修正機能とは、NTP（Network Time Protocol）を使って、インターネット上の正確な時刻を保持しているサーバと通信して、本製品の内蔵時計を正確に合わせる機能です。

●自動時刻修正

時刻修正機能を使うかどうかを選択します。

◆しない

時刻修正機能は使用しません。
本製品の時刻は、［設定する日付けと時刻］で設定して下さい。

◆する

時刻修正機能を使用します。

●NTPサーバアドレス（プライマリ）/（セカンダリ）

時刻を問い合わせるNTPサーバのIPアドレスを入力します。購入時は［133.100.9.2］に設定されています。
※IPアドレスは、ドットノーテーション（XXX.XXX.XXX.XXXの形式）で入力します。

●NTPサーバへの経由先

時刻を問い合わせるNTPサーバにアクセスするために経由する相手先を選択します。

PPPoE（端末型）接続、またはPPPoE（LAN型）接続で設定したときは、そのプロバイダを登録した相手先の番号を選択します。LAN内のNTPサーバにアクセスするときや、PPPoEを使用していないプロバイダを経由するときは、［Ethernet］を選択します。

●修正する間隔

時刻を自動的に修正する日数間隔を、半角数字1～7の範囲で入力します。

●次回修正予定日時

次にNTPサーバにアクセスして、時刻を修正する予定が表示されています。

予定に関わらず、時刻を直ちに修正したいときは、［今すぐ修正］ボタンをクリックします。NTPサーバへのアクセスが相手先を経由する場合は、その相手先と接続している必要があります。

時刻が未設定の状態（年が1996）の場合、LAN上にNTPサーバがない場合は初めて回線を接続したときに、設定されているNTPサーバへ時刻の問い合わせが行われます。正常に通信ができると自動的に時刻が修正されます。

WAN

ブロードバンドを使用し、CATVインターネットやPPPoEを採用していないプロバイダと接続するときに必要な設定を行います。

● ［設定］ボタン/［やり直し］ボタン
　設定を有効にするときは、［設定］ボタンをクリックします。
　設定をやり直すときは、［やり直し］ボタンをクリックします。入力した内容が消去されます。

［設定］ボタンをクリックせずに他のページを開くと、設定した内容は消去されます。

■基本

●IPアドレス
　WANポートのIPアドレスをプロバイダのDHCPサーバから取得するか、あらかじめ通知されたIPアドレスを手動で入力するかを選択します。プロバイダの指示に従って下さい。購入時は［DHCPサーバから取得］に設定されています。

◆DHCPサーバから取得
　DHCPサーバから取得するときに、選択します。

◆固定IP（DHCPをOFF）
　プロバイダから通知されているIPアドレスを手動で入力するときに､選択します。

●DHCPクライアントID
　IPアドレスをプロバイダのDHCPサーバから取得している場合で、クライアントIDが指定されているときは、そのIDを入力します。指定されていないときは、空白にして下さい。

●MTUサイズ
　WANポートのMTUの値を設定します。
　本製品の初期設定のMTUサイズ（1500byte）では、うまく通信できないときにMTUのサイズを変更します。540～1500の範囲で設定して下さい。

■固定IP

●IPアドレス/サブネットマスク長
　プロバイダから通知されているIPアドレスとサブネットマスク長を入力します。

●DNSサーバアドレス（プライマリ）/（セカンダリ）
　プロバイダから通知されているDNSサーバアドレスを入力します。

●ゲートウェイアドレス
　プロバイダから通知されているゲートウェイアドレスを入力します。

■オプション

ルータ機能に関する設定には、ここでコマンドを入力して設定するものがあります。入力欄をクリックするとカーソルが表示されるので、コマンドを入力して下さい。コマンドを入力する際は、以下の点を注意して下さい。

- { }で囲まれている部分がパラメータです。パラメータの区切りには、半角スペースを入力します。パラメータによっては「/」（スラッシュ）が必要なものがあります。
- 太字は、購入時の値を意味します。
- ［　］内はオプションです。付けても付けなくても構いません。
- オプション以外のパラメータを省略すると、設定できません。
- 複数のコマンドを設定するときは、コマンドごとに改行して下さい。

●WAN側接続モード設定

ブロードバンドを使用し、CATVインターネットやPPPoEを採用していないプロバイダと接続するときに、LAN内の端末にグローバルIPアドレスを設定し、NAT変換を行わない環境を構築できます。

書式　wan ether ip mode {mode}

パラメータ　{mode}

lan：LAN型接続

terminal：端末型接続

設定例　200.200.200.129/29の複数アドレスの払い出しを受けた場合（デフォルトゲートウェイの指定が200.200.200.1）

- WAN設定－［基本］－［IPアドレス］：固定IP（DHCPをOFF）
- WAN設定－［固定IP］－［IPアドレス/サブネットマスク長］：200.200.200.129/24

※サブネットマスク長はデフォルトゲートウェイが含まれるような値を設定します。

- WAN設定－［固定IP］－［DNSサーバアドレス（プライマリ）/（セカンダリ）］：プロバイダから通知されているDNSサーバアドレスを入力します。
- WAN設定－［固定IP］－［ゲートウェイアドレス］：200.200.200.1
- WAN設定－［オプション］：wan ether ip mode lan
- LAN設定－［基本］－［本体のIPアドレス/サブネットマスク長］：200.200.200.129/29

LAN

本製品のLAN側の設定を行います。

「"」(ダブルクォーテーション)と半角スペースを続けて設定欄に入力することはできません。

● [設定] ボタン/ [やり直し] ボタン
設定を有効にするときは、[設定] ボタンをクリックします。
設定をやり直すときは、[やり直し] ボタンをクリックします。入力した内容が消去されます。

[設定] ボタンをクリックせずに他のページを開くと、設定した内容は消去されます。

■基本

●本体のIPアドレス/サブネットマスク長
本製品のIPアドレスとサブネットマスク長を入力します。購入時は [192.168.1.1/24] に設定されています。
※IPアドレスは、ドットノーテーション(XXX.XXX.XXX.XXXの形式)で入力します。

●ブロードキャストアドレス
LAN上のすべてのパソコンにパケットを送信することがあります。そのときに使うIPアドレスを「ブロードキャストアドレス」といいます。
ブロードキャストアドレスを選択します。詳しくは、ネットワークの管理者に相談して下さい。購入時は [全て1] に設定されています。

◆全て0
ブロードキャストアドレスとして「0」(ゼロ)を指定する必要があるLAN上で、すべてのパソコンにパケットを送信します。

◆全て1
ブロードキャストアドレスとして「1」を指定します。通常は、[全て1] の設定で構いません。

◆サブネット+全て0
ブロードキャストアドレスとして「0」(ゼロ)を指定する必要があるLAN上で、特定のサブネットのすべてのパソコンにパケットを送信します。

◆サブネット+全て1
ブロードキャストアドレスとして「1」を指定して、特定のサブネットのすべてのパソコンにパケットを送信します。

●RIP送受信モード

RIP（Routing Information Protocol）のモードを設定します。
RIPを送信する設定にすると、約30秒ごとにRIPパケットがLAN上のすべてのパソコンに送信されます。購入時は［送信と受信を行う］に設定されています。

◆送信と受信を行う

RIPのパケットを送受信します。

◆送信も受信も行わない

RIPのパケットの送受信は行いません。LAN上のすべてのパソコンにRIPを送信することはなく、受信したRIPは無視します。

◆受信のみ行う

RIPパケットの受信のみ行います。

◆送信のみ行う

RIPパケットの送信のみ行います。

●MTUサイズ

LANポートのMTUの値を設定します。
本製品の初期設定のMTUサイズ（1500byte）では、うまく通信できないときにMTUのサイズを変更します。540〜1500の範囲で設定して下さい。

■DHCPサーバ

DHCPサーバ機能とは、LAN上のパソコンにIPアドレスを自動的に設定する機能です。

●DHCPサーバ機能

DHCPサーバ機能を使うかどうか選択します。購入時は［ON］に設定されています。

◆OFF

本製品からIPアドレスを割り当てません。
既存のLANに本製品を導入するときなどで、すでにLAN上にDHCPサーバがある場合や、IPアドレスを手動で設定する場合は、OFFにします。

◆ON

本製品からIPアドレスを割り当てます。
ONにするときは、［開始IPアドレス/個数］にパソコンに設定するIPアドレスの範囲を入力して下さい。

●開始IPアドレス/個数

DHCPサーバ機能を使ってパソコンに設定するIPアドレスの範囲を入力します。割り当てる先頭のIPアドレスと、個数を入力して下さい。購入時は［192.168.1.2/32］に設定されています。

※設定するときは、次のことに注意して下さい。
　本製品と同じサブネットのIPアドレスを設定すること
　本製品のIPアドレスと重複しないように設定すること

●ドメイン名

DHCPサーバ機能を使うとき、LAN上で使用しているドメイン名を入力します。IPアドレスと共にドメイン名も各パソコンに設定されます。
特に必要がない限り、ドメイン名を設定する必要はありません。

◆DHCPでIPアドレスを割り当てるプロバイダに接続する場合

DHCPでIPアドレスを自動的に割り当てるプロバイダに接続するときは、ドメイン名も取得できることがあります。その場合、[ドメイン名]が空欄のときだけ、プロバイダから取得したドメイン名がパソコンに通知されます。

●リース時間

DHCPサーバ機能を使って設定されるIPアドレスの有効期限（1～9999時間）を入力します。購入時は[24]時間に設定されています。
ここで設定した時間を経過すると、一度設定されたIPアドレスが再利用できるようになります。

◆パソコンに割り当てられたIPアドレスの更新

DHCPサーバ機能によってパソコンに設定されたIPアドレスは、[リース時間]が経過するまで使用されます。本製品のIPアドレスを変更したときなどパソコンのIPアドレスの変更が必要な場合でも、IPアドレスは自動的に更新されません。
[リース時間]内にパソコンに新しいIPアドレスを設定する場合は、それぞれのパソコンで操作して下さい。

●WINSサーバアドレス（プライマリ）/（セカンダリ）

DHCPサーバ機能を使用するとき、パソコンに割り当てるWINSサーバのIPアドレスを設定します。

※IPアドレスは、ドットノーテーション（XXX.XXX.XXX.XXXの形式）で入力します。

LAN上のWindows XP/2000/MeのTCP/IPの設定で「WINSの解決にDHCPを使う」にしておくと、DHCPサーバからIPアドレスを取得する際に、ここで設定するWINSサーバアドレスが自動的に設定されます。

■AutoDNS

AutoDNS機能とは、プロバイダ側のDNSサーバアドレスを検出したり、パソコンからのドメイン名解決要求をDNSサーバへ転送したりする機能です。ここの設定のほかに、LAN上のパソコンで必要な設定を行うと、異なるプロバイダに接続するたびにDNSサーバの設定を変更する必要がなくなります。

●AutoDNS機能

AutoDNS機能を使うかどうか選択します。購入時は[ON]に設定されています。

◆OFF

AutoDNS機能は使用しません。

◆ON

AutoDNS機能を有効にします。
接続先のDNSサーバを利用する場合はとくに、AutoDNS機能を使うことをお勧めします。

AutoDNS機能を使用する場合、LAN上のパソコンで本製品のIPアドレスをDNSサーバアドレスとして設定して下さい。

●LAN側DNSサーバアドレス（プライマリ）/（セカンダリ）

LANにDNSサーバがあるときに設定する項目です。

AutoDNS機能を使用するとき、パソコンからのドメイン名解決要求を転送したいDNSサーバのIPアドレスを入力します。

［AutoDNS機能］をONにしている場合は、LAN上のDNSサーバのIPアドレスを入力します。

また、［AutoDNS機能］をOFF、［DHCPサーバ機能］をONにしている場合は、LAN上または相手先のDNSサーバのIPアドレスを入力します。

設定したIPアドレスが、DNSサーバのアドレスとして各パソコンに通知されます（プライマリのみ）。

■オプション

ルータ機能に関する設定には、ここでコマンドを入力して設定するものがあります。入力欄をクリックするとカーソルが表示されるので、コマンドを入力して下さい。コマンドを入力する際は、以下の点を注意して下さい。

・{ }で囲まれている部分がパラメータです。パラメータの区切りには、半角スペースを入力します。パラメータによっては「/」（スラッシュ）が必要なものがあります。

・太字は、購入時の値を意味します。

・［　］内はオプションです。付けても付けなくても構いません。

・オプション以外のパラメータを省略すると、設定できません。

・文字列がパラメータとなる場合で、そのパラメータがスペースを含んでいるときは文字列を ""で囲んで入力して下さい。

（例）「ab cd」をパラメータとして入力するときは、"ab cd"と入力します。

・複数のコマンドを設定するときは、コマンドごとに改行して下さい。

●ホスト情報登録（DHCPスタティック機能／簡易DNS機能の設定）

パソコンのホスト名とIPアドレス、Ethernet（MAC）アドレスの組み合わせを登録します。ホスト情報は32件まで登録することができます。ここで登録した内容は次の場合に使用されます。

◆DHCPスタティック機能

パソコンのMACアドレスに対してDHCPで割り当てるIPアドレスを指定することができます。この機能を使うことで、DHCPであってもいつも同じパソコンに同じIPアドレスを割り当てることが可能です。

◆簡易DNS機能

本製品がDNSサーバのように動作し、パソコンからのドメイン名解決要求やドメイン名逆引き要求に応じて応答する機能です。ホスト名のほかエイリアス名を指定することもできます。

どちらの場合も、設定は次のように行います。

詳細設定編

書式　　　**ip host {ipaddress} {name}[[{alias}] {macaddress}]**

パラメータ　{ipaddress}：パソコンのIPアドレス

※ドットノーテーション（XXX.XXX.XXX.XXXの形式）で入力します。

{name}：パソコンのホスト名
{alias}：パソコンのホスト名（エイリアス名）
{macaddress}：Ethernet（MAC）アドレス

※XX:XX:XX:XX:XX:XXの形式で入力します。

●IP経路情報の登録

IP経路情報を追加登録します。IP経路情報は32個まで登録できます。登録した経路がすでにIP経路情報に存在する場合は追加されません。
IP経路情報を登録する書式は、WAN側（PPPoEを使用するブロードバンド）の場合、WAN側（PPPoEを使用しないブロードバンド）の場合、LAN側の場合で異なります。

書式

1）LAN側の経路の場合
ip route {net}/{mask}/{hops} local {gateway}

2）WAN側（PPPoEを使用するブロードバンド）の経路の場合
ip route {net/mask}/{hops} remote {rnumber} {type}

3）WAN側（PPPoEを使用しないブロードバンド）の経路の場合
ip route {net}/{mask}/{hops} wanether

パラメータ

1）LAN側の経路の場合
{net}：ネットワーク番号またはサブネットワーク番号

※ドットノーテーション（XXX.XXX.XXX.XXXの形式）で入力します。

{mask}：サブネットマスクまたはマスクビット数

※サブネットマスクは、ドットノーテーション（XXX.XXX.XXX.XXXの形式）で入力します。

{hops}=1～15：ホップカウント
{gateway}：ゲートウェイのIPアドレス

2）WAN側（PPPoEを使用するブロードバンド）の経路の場合
{net}：ネットワーク番号またはサブネットワーク番号

※ドットノーテーション（XXX.XXX.XXX.XXXの形式）で入力します。

{mask}：サブネットマスクまたはマスクビット数

※サブネットマスクは、ドットノーテーション（XXX.XXX.XXX.XXXの形式）で入力します。

{hops}=1～15：ホップカウント
{rnumber}=0～7：相手先番号（登録番号#0～#7）
{type}
auto：経路情報種別－自動接続ルート（自動接続する）
static：経路情報種別－スタティックルート（自動接続しない）

3）WAN側（PPPoEを使用しないブロードバンド）の経路の場合
{net}：ネットワーク番号またはサブネットワーク番号

※ドットノーテーション（XXX.XXX.XXX.XXXの形式）で入力します。

{mask}：サブネットマスクまたはマスクビット数

※サブネットマスクは、ドットノーテーション（XXX.XXX.XXX.XXXの形式）で入力します。

{hops}=1～15：ホップカウント

設定例　1）LAN側の場合
IPアドレス「192.168.1.100」のルータを経由するデフォルトルート（ホップカウント「7」）を登録するとき
→　ip route 0.0.0.0/0/7 local 192.168.1.100

2）WAN側（PPPoEを使用するブロードバンド）の場合
相手先#1のネットワーク番号「172.16.0.0/16」をスタティックルート（ホップカウント「2」）として登録するとき
→　ip route 172.16.0.0/16/2 remote 1 static

※クイック設定→［ブロードバンドでの接続］→［PPPoE（端末型）］画面［PPPoE（LAN型）］画面で設定すると、下記のコマンドが自動的に設定されます。
ip route 0.0.0.0/0/7 remote 0,1 auto
または
ip route 0.0.0.0/0/7 remote 0 auto
または
ip route 0.0.0.0/0/7/ remote 1 auto

●IPフィルタの登録

フィルタを登録します。最大64個のフィルタを登録できます。
フィルタを登録すると、本製品が受信したパケットごとにフィルタと比較します。比較は、フィルタ番号の小さいフィルタから順に行われ、パケットは最初に該当したフィルタの条件に従って処理されます。該当するフィルタがないパケットは通過します。
また、フィルタが登録されていない場合は、すべてのアクセスが許可されます。
IPフィルタを登録する書式は、LAN側の場合、WAN側（PPPoEを使用するブロードバンド）の場合、WAN側（PPPoEを使用しないブロードバンド）の場合で異なります。

書式　1）LAN側のフィルタ（TCPまたはUDP）の場合
ip filter {fnumber} {type} {dir} {srcaddr} {dstaddr} {protocol} {srcport} {dstport} local [nolog]

2）WAN側（PPPoEを使用するブロードバンド）のフィルタ（TCPまたはUDP）の場合
ip filter {fnumber} {type} {dir} {srcaddr} {dstaddr} {protocol} {srcport} {dstport} remote {rnumber} [nolog]

3）LAN側のICMPフィルタの場合
ip filter {fnumber} {type} {dir} {srcaddr} {dstaddr} icmp {icmptype} local [nolog]

4）WAN側（PPPoEを使用するブロードバンド）のICMPフィルタの場合
ip filter {fnumber} {type} {dir} {srcaddr} {dstaddr} icmp {icmptype} remote {rnumber} [nolog]

5）LAN側のフィルタ（TCPまたはUDP以外）の場合
ip filter {fnumber} {type} {dir} {srcaddr} {dstaddr} {protocol} local [nolog]

6）WAN側（PPPoEを使用するブロードバンド）のフィルタ（TCPまたはUDP以外）の場合
ip filter {fnumber} {type} {dir} {srcaddr} {dstaddr} {protocol} remote {rnumber} [nolog]

7）WAN側（PPPoEを使用しないブロードバンド）のフィルタ（TCPまたはUDP）の場合
ip filter {fnumber} {type} {dir} {srcaddr} {dstaddr} {protocol} {srcport} {dstport} wanether [nolog]

8）WAN側（PPPoEを使用しないブロードバンド）のフィルタ（TCPまたはUDP以外）の場合
ip filter {fnumber} {type} {dir} {srcaddr} {dstaddr} {protocol} wanether [nolog]
9）WAN側（PPPoEを使用しないブロードバンド）のICMPフィルタの場合
ip filter {fnumber} {type} {dir} {srcaddr} {dstaddr} icmp {icmptype} wanether [nolog]
10）全てのWAN側のフィルタ（TCPまたはUDP）の場合
ip filter {fnumber} {type} {dir} {srcaddr} {dstaddr} {protocol} {srcport} {dstport} wanany [nolog]
11）全てのWAN側のフィルタ（TCPまたはUDP以外）の場合
ip filter {fnumber} {type} {dir} {srcaddr} {dstaddr} {protocol} wanany [nolog]
12）全てのWAN側のICMPフィルタの場合
ip filter {fnumber} {type} {dir} {srcaddr} {dstaddr} icmp {icmptype} wanany [nolog]

パラメータ
{fnumber}=1～64：フィルタ番号
{type}
pass：フィルタタイプ－転送する
reject：フィルタタイプ－破棄する
restrict：フィルタタイプ－回線が接続されている場合、一致すれば通す
{dir}
in：方向－受信時にフィルタリングする
out：方向－送信時にフィルタリングする
{srcaddr}：{送信元ネットワーク番号または送信元サブネットワーク番号}[/{サブネットマスクまたはマスクビット数}]または[-{送信元アドレスの範囲}]
※送信元ネットワーク番号、送信元サブネットワーク番号、送信元アドレス、サブネットマスクは、ドットノーテーション（XXX.XXX.XXX.XXXの形式）で入力します。
※送信元アドレスを範囲指定する場合は、開始と終了の送信元アドレスを「-」で区切ってください。
※「*」を設定すると、すべての送信元が対象になります。

{dstaddr}：{送信先ネットワーク番号または送信先サブネットワーク番号}[/{サブネットマスクまたはマスクビット数}]または[-{送信先アドレスの範囲}]
※送信先ネットワーク番号、送信先サブネットワーク番号、送信先アドレス、サブネットマスクは、ドットノーテーション（XXX.XXX.XXX.XXXの形式）で入力します。
※送信先アドレスを範囲指定する場合は、開始と終了の送信先アドレスを「-」で区切ってください。
※「*」を設定すると、すべての送信先が対象になります。

{protocol}：プロトコル番号またはニーモニック
※ニーモニックは、次のものがあります。
「esp」「gre」「icmp」「ipencap」「tcp」「tcpest」「tcpfin」「udp」「tcp_udp」
※「*」を設定すると、すべてのプロトコルが対象になります。

{srcport}：送信元ポート番号またはニーモニック
※プロトコルに「tcp」「tcpest」「tcpfin」「udp」「tcp_udp」を指定したときは送信元ポート番号またはニーモニックを指定します。
※送信元ポート番号を範囲指定する場合は、開始と終了の送信元ポート番号を「-」で区切ってください。
※ニーモニックは、次のものがあります。
「ftp」「ftpdata」「telnet」「smtp」「www」「pop3」「sunrpc」「nntp」「ntp」「login」「pptp」「domain」「route」「who」
※「*」を設定すると、すべての送信元ポート番号またはニーモニックが対象になります。

{dstport}：送信先ポート番号またはニーモニック

※送信先ポート番号を範囲指定する場合は、開始と終了の送信先ポート番号を「-」で区切ってください。
※ニーモニックは、次のものがあります。
「ftp」「ftpdata」「telnet」「smtp」「www」「pop3」「sunrpc」「nntp」「ntp」「login」「pptp」「domain」「route」「who」
※「*」を設定すると、すべての送信先ポート番号またはニーモニックが対象になります。

{icmptype}：ICMPタイプ

※protocolに「icmp」を指定したときはICMPタイプを指定します。
0...エコー応答（Echo Reply）
3...到達不能（Destination Unreachable）
4...発信抑制（Source Quench）
5...ルート変更（Redirect）
8...エコー（Echo）
9...ルータ通知（Router Advertisement）
10...ルータ選択（Router Selection）
11...時間超過（Time Exceeded）
12...パラメータ異常（Parameter Problem）
13...タイムスタンプ（Timestamp）
14...タイムスタンプ応答（Timestamp Reply）
15...情報要求（Information Request）
16...情報応答（Information Reply）
17...アドレスマスク要求（Address Mask Request）
18...アドレスマスク応答（Address Mask Reply）
30...トレースルート（Traceroute）
37...ドメイン名要求（Domain Name Request）
38...ドメイン名応答（Domain Name Reply）

{rnumber}=0〜7,*：相手先番号（登録番号#0〜#7）

※「*」を設定すると、すべての相手先が対象になります。

設定例

1）相手先#1と接続している場合、IPアドレス「192.168.10.10」の機器に対する、ftpによるアクセスを禁止するとき（フィルタ番号1に登録）
→ ip filter 1 reject in * 192.168.10.10 tcp * ftp remote 1

2）相手先#2に端末型ダイヤルアップ接続している場合、アクセスできるパソコンを「192.168.10.10」〜「192.168.10.19」に限定するとき（フィルタ番号2、3に登録）
→ ip filter 2 pass out 192.168.10.10-192.168.10.19 * * remote 2
→ ip filter 3 reject out * * * remote 2

3）TCP/SMTPパケットをLAN側からWAN側に送信する際、このフィルタを通過したパケットのログを出力しないとき（フィルタ番号4に登録）
→ ip filter 4 pass out * * tcp * smtp remote * nolog

ポートの概念がないプロトコル（TCPやUDP以外のプロトコル）の場合、ポート番号は設定できません。
例）ip filter 1 reject in 172.16.10.1 192.168.10.1 gre remote 0
上記のフィルタを設定した場合、172.16.10.1から192.168.10.1へ送信されるGREパケットは破棄されます。
すべてのプロトコルを対象とするフィルタを設定した場合、プロトコルによらずポートの概念を無視して設定されます。
例）ip filter 1 reject in 172.16.10.1 192.168.10.1 * * * remote 0
上記のフィルタを設定した場合、送信されるプロトコルによって、次のようになります。
・172.16.10.1から192.168.10.1へTCPやUDPのパケットを送信した場合
このフィルタが適用され、すべてのパケットが破棄されます。

・172.16.10.1から192.168.10.1へGREやICMPのパケットを送信した場合
　このフィルタが適用され、すべてのパケットが破棄されます。
　プロトコルとしてtcp_udpのフィルタを設定した場合、TCPとUDPの場合にポート番号によるフィルタリングが可能です。

例）ip filter 1 reject in 172.16.10.1 192.168.10.1 tcp_udp * 1000 remote 0
　上記のフィルタを設定した場合、送信されるプロトコルによって、次のようになります。

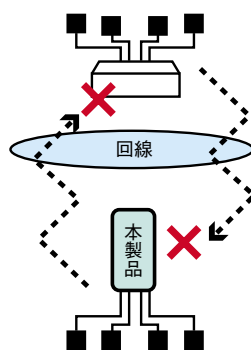
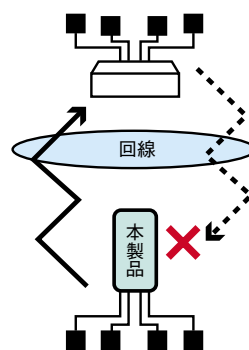
・172.16.10.1から192.168.10.1へTCPやUDPのパケットを送信した場合
　送信先ポートが1000番で一致した場合のみ、このフィルタが適用され、パケットが破棄されます。
・172.16.10.1から192.168.10.1へGREやICMPのパケットを送信した場合
　一致しない為、パケットは破棄されません。

◆プロトコル「TCP」「TCPEST」の違いについて

「IPフィルタの登録」では、{protocol}（プロトコル）に「TCP」「TCPEST」を設定することができます。
「TCP」を設定すると、TCPのセッションによるすべてTCPのパケットが対象になります。「TCPEST」を設定すると、TCPのセッションを張る際の最初のTCPパケットだけが対象になります。
次の例を参考にして下さい。

・TCPの場合
　ip filter 1 reject in * * tcp * * remote 0
　→ 相手先からのTCPパケットをすべて破棄します。TCPによるすべての通信が不可能になります。
・TCPESTの場合
　ip filter 1 reject in * * tcpest * * remote 0
　→相手先からは、TCPを使用するすべての通信サービスを利用できません。
　ただし、こちら側からは、TCPを使用するすべての通信サービスを利用できます。

TCPESTの場合

詳細設定編

●IPフィルタの登録（拡張）

DNS Queryパケットに関するIPフィルタを登録します。通常のIPフィルタとあわせて最大64個のフィルタを登録できます。

フィルタを登録すると、本製品が受信したDNS Queryパケットごとにフィルタと比較します。比較は、フィルタ番号の小さいフィルタから順に行われ、DNS Queryパケットは最初に該当したフィルタの条件に従って処理されます。該当するフィルタがないDNS Queryパケットは通過します（転送されます）。また、フィルタが登録されていない場合は、すべてのDNS Queryパケットが通過します（転送されます）。

書式　**ip filter {fnumber} {type} dns qtype {number} [nolog]**

パラメータ　{fnumber}=1～64：フィルタ番号

{type}

pass：フィルタタイプ－一致すれば転送する

reject：フィルタタイプ－一致すれば破棄する

{number}：クエリタイプ番号

nolog：このフィルタに対するログを出力しない

［IPフィルタの登録（拡張）］でクエリタイプ番号「1」または「12」を破棄する設定にすると、本製品は簡易DNSサーバになりません。

代表的なクエリタイプ番号

番号	コード	内容
1	A	ホストアドレス
2	NS	そのドメインのオーソリティネームサーバ
3	MD	そのドメインのメールエージェントを持つホストを示す
4	MF	そのドメインのためにメールを送信できるホストを示す
5	CNAME	エイリアスの標準名
6	SOA	オーソリティゾーンの起点
7	MB	指定されたメールボックスを持つホストを示す
8	MG	そのメールグループに属するメールボックスを示す
9	MR	改名メールボックスのドメイン名
10	NULL	その他の情報
11	WKS	ウェルノウンサービス記述
12	PTR	ドメイン名スペースの他の部分へのポインタ
13	HINFO	そのホストが使うCPUとオペレーティングシステムのタイプ
14	MINFO	メーリングリストを担当するメールボックス
15	MX	そのドメインのメール交換局
16	TXT	単なるテキスト文字列

●IPアドレス変換（NAT）テーブルの登録

IPアドレス変換（NAT）テーブルを登録します。最大32個のNATテーブルを登録できます。

NATテーブルを登録すると、本製品が受信したパケットのIPアドレスごとにNATテーブルと比較します。比較は、NATテーブル番号の小さな順に行われ、該当するNATテーブルに従ってIPアドレスが変換されます。（ポート番号も指定して変換可能）

NATテーブルを1個でも登録すると、該当するNATテーブルがないIPアドレスは、通信できなくなります。

IPアドレス変換（NAT）テーブルを登録する書式は、WAN側（PPPoEを使用しているブロードバンド）の場合、WAN側（PPPoEを使用していないブロードバンド）の場合、WAN側（PPPoEを使用しているブロードバンド）とWAN側（PPPoEを使用していないブロードバンド）両方の場合で異なります。

書式

1）WAN側（PPPoEを使用しているブロードバンド）の場合

ip nat {nnumber} {private}[/{protocol}/{p_port}] {global}[/{g_port}] remote [{rnumber}] [latest]

2）WAN側（PPPoEを使用していないブロードバンド）の場合

ip nat {nnumber} {private} [/{protocol}/{p_port}] {global}[/{g_port}] wanether [latest]

3）WAN側（PPPoEを使用しているブロードバンド）とWAN側（PPPoEを使用していないブロードバンド）両方の場合

ip nat {nnumber} {private} [/{protocol}/{p_port}] {global}[/{g_port}] * [{rnumber}] [latest]

パラメータ

{nnumber}=1～32：NATテーブル番号

{private}：プライベートIPアドレス

※ドットノーテーション（XXX.XXX.XXX.XXXの形式）で入力します。
※プライベートIPアドレスの範囲を指定する場合は、開始と終了のプライベートIPアドレスを「-」で区切って下さい。
※「*」を設定すると、すべてのIPアドレスが対象になります。

{protocol}：プロトコル

※プロトコルは、次のものがあります。
「udp」「tcp」「gre」「icmp」「ipencap」「esp」「tcp_udp」
※「*」を設定すると、すべてのプロトコルが対象になります。
※{port}と合わせて、省略できます。省略した場合は、すべてのプロトコルが対象になります。

{p_port}：プライベートポート番号またはニーモック

※ニーモニックは、次のものがあります。
「ftp」「ftpdata」「telnet」「smtp」「www」「pop3」「sunrpc」「nntp」「ntp」「login」「domain」「pptp」「route」「who」
※ポート番号またはニーモニックの範囲を指定する場合は、開始と終了のポート番号またはニーモニックを「-」で区切って下さい。
※「*」を設定すると、すべてのポート番号またはニーモニックが対象になります。
※「*」を設定するとポート番号の設定は無視されます。TCP/UDP通信に対して同じポート番号のNATテーブルを設定する場合は、「tcp_udp」を設定するようにして下さい。

詳細設定編

{global}：グローバルIPアドレス

※ドットノーテーション（XXX.XXX.XXX.XXXの形式）で入力します。
※WANポートを使って通信する場合、IPアドレスを手動で入力で設定したときは、同じIPアドレスを入力します。
※「ipcp」を設定すると、PPPoEを採用しているプロバイダに接続する場合に割り当てられるIPアドレスになります。
※「dhcp」を設定すると、WANポートを使ったIP通信時に使用するIPアドレスになります。
※「dynamic」を設定すると、PPPoEを採用しているプロバイダに接続する場合に割り当てられるIPアドレス、あるいは、WANポートを使ったIP通信時に使用するIPアドレスになります。
※「*（すべて）」を設定することはできません。
※「ipcp」「dhcp」「dynamic」を設定すると、その設定内容に関わらず、[情報表示（設定）] 画面では次のように表示されます。
WAN側（接続相手先）の場合：「ipcp」
WAN側（WANポート）の場合：「dhcp」
WAN側（接続相手先）とWAN側（WANポート）両方の場合：「dynamic」

{g_port}：グローバルポート番号またはニーモック

※ニーモックには、次のようなものがあります。
「ftp」「ftpdata」「telnetl」「smtp」「www」「pop3」「sunrpc」「nntp」「ntp」「login」「domain」「pptp」「route」「who」
※「*」を指定するとポート番号の設定は無視されます。

{rnumber}=0〜7,*：相手先番号（登録番号#0〜#7）

※WAN側（接続相手先）の場合、「*」を設定すると、すべての相手先が対象になります。また、省略した場合も、すべての相手先が対象になります。
※「0〜7、*」のいずれかを設定すると、その設定した相手先が対象になります。

latest：latestオプションの使用

※プライベートIPアドレスで、すべてのIPアドレスが指定されているか、IPアドレスの範囲が指定されている場合に有効です。
※latestオプションは、設定された複数のプライベートIPアドレスのうち、最後に通信したプライベートIPアドレスに変換します。設定されているプロトコルおよびポート番号のすべてにWAN側からのアクセスが可能になります。

設定例

1）相手先＃1にLAN型接続している場合、グローバルIPアドレス「133.232.200.90」を使用してアクセスできるパソコンを「192.168.0.2」に限定するとき（NATテーブル番号1に登録）
→ ip nat 1 192.168.0.2/*/* 133.232.200.90 remote 1

2）相手先#2に端末型接続している場合、外部にアクセスできるパソコンを「192.168.10.10」〜「192.168.10.19」に限定するとき（NATテーブル番号2に登録）
→ ip nat 2 192.168.10.10-192.168.10.19 ipcp remote 2

3）CATVインターネットやADSLのPPPoEを採用していないプロバイダに接続してインターネットにアクセスする場合、通信時に割り当てられるグローバルIPアドレスを使って、「192.168.10.10」〜「192.168.10.19」のパソコンがアクセスするとき（NATテーブル番号3に登録）
→ ip nat 3 192.168.10.10-192.168.10.19 dhcp wanether

◆latestオプションを使用すると、NATテーブルに登録されていないパケットをWAN側から受信した場合、最後に通信を行ったプライベートIPアドレスに転送します。設定されているプロトコルおよびポート番号のすべてに外部からのアクセスが可能になりますので、latestオプションを使用するのは、どうしても必要な場合だけにして下さい。

◆グローバルポート番号を指定した場合は、プライベートIPアドレス、プロトコル、プライベートポート番号を一意に設定する必要があります。プロトコルをTCPまたはUDP以外に設定したり、IPアドレスの指定を省略または範囲指定にすることはできません。

●NAT使用時のブロードキャストパケット転送の設定

NAT使用時にWAN側から受信したブロードキャストパケットをLAN側へ転送するかどうかを設定します。
転送するときは、ブロードキャストパケットの送信先のIPアドレスが、LAN側のブロードキャストアドレスに変換されます。

書式　**ip natbcast {on｜off}**
パラメータ　{on｜off}
off：NAT使用時にブロードキャストパケットを転送しない
on：NAT使用時にブロードキャストパケットを転送する

NAT使用時にブロードキャストパケットを転送する設定にすると、NATテーブルの内容にかかわらず、すべてのブロードキャストパケットが転送されます。

●Directed-Broadcastの設定

LAN型接続時に、Directed-Broadcastを転送するかどうかを設定します。

書式　**ip drctbcast {mode}**
パラメータ　{mode}
forward：Directed-Broadcastの動作モードー転送する
discard：Directed-Broadcastの動作モードー破棄する

詳細設定編

ルータ

WAN側から本製品のルータへのアクセス制限の設定、VPN（仮想プライベートネットワーク）のパケットを透過させる設定を行います。

● ［設定］ボタン/［やり直し］ボタン
設定を有効にするときは、［設定］ボタンをクリックします。
設定をやり直すときは、［やり直し］ボタンをクリックします。入力した内容が消去されます。

［設定］ボタンをクリックせずに他のページを開くと、設定した内容は消去されます。

■VPNパススルー設定

LAN内のVPNクライアントまたはサーバのパケットを、WAN側へ通過させる機能です。この機能を利用すると、IPアドレス変換（NAT）テーブルを設定しなくても、LAN内のパソコンがVPNを使用して、外部の機器と通信が可能になります。対応しているVPNのプロトコルは、IPsec、PPTP、L2TPです。購入時はすべての項目で［透過しない］に設定されています。
※ IPsecを利用する場合、LAN側の複数の端末から同じ通信相手に対し同時に通信できません。

●IPsecパススルー
◆透過しない
IPsecのパケットを透過しません。
◆透過する
IPsecのパケットを透過します。

●LAN側IPsecホストアドレス
特定のパソコンでだけIPsecで通信するとき、そのパソコンのIPアドレスを入力します。ほかのパソコンで、IPsecの通信はできなくなります。
LAN内にIPsecのサーバを設置するときは、必ずサーバのIPアドレスを入力して下さい。

●PPTPパススルー
◆透過しない
PPTPのパケットを透過しません。
◆透過する
PPTPのパケットを透過します。

●LAN側PPTPホストアドレス
特定のパソコンでだけPPTPで通信するとき、そのパソコンのIPアドレスを入力します。ほかのパソコンで、PPTPの通信はできなくなります。
LAN内にPPTPのサーバを設置するときは、必ずサーバのIPアドレスを入力して下さい。

●L2TPパススルー
◆透過しない
L2TPのパケットを透過しません。
◆透過する
L2TPのパケットを透過します。

●LAN側L2TPホストアドレス
特定のパソコンでだけL2TPで通信するとき、そのパソコンのIPアドレスを入力します。ほかのパソコンで、L2TPの通信はできなくなります。
LAN内にL2TPのサーバを設置するときは、必ずサーバのIPアドレスを入力して下さい。

■ステルスモード設定

本製品をステルスモードにすると、WAN側から本製品に対して送信されたPINGコマンドに応答しません。また、WAN側にICMPエラー、TCPリセット（ただしポート番号113を除く）も返さなくなります。購入時［ステルスモード］の設定は［ON］、［ログ出力］の設定は［する］に設定されています。

●ステルスモード
◆ON
ステルスモードで動作します。
◆OFF
通常のモードで動作します。WAN側からのPINGコマンドに応答します。

●ログ出力
ステルスモードにして、応答せずに破棄したパケットのログを［情報表示］→［ログ］に出力できます。
◆する
ログを出力します。

破棄したパケットのログを出力するときは、［セキュリティ設定］→［ログ通知］で［NOTICE］をチェックして下さい。

◆しない
ログを出力しません。

■SPI設定

SPI（Stateful Packet Inspection：ステートフル・パケット・インスペクション）は、通信の状態を監視して、送受信パケットの矛盾や異常をチェックする機能です。LAN側からの通信状態の予測に基づいて受信パケットを検査し、不正なパケットと判断された場合にはそのパケットを破棄します。購入時［SPI］の設定は［ON］、［ログ出力］の設定は［する］に設定されています。

●SPI

◆ON

SPI機能を有効にします。

◆OFF

SPI機能を無効にします。

●ログ出力

SPI機能で破棄したパケットのログを［情報表示］→［ログ］に出力できます。

◆する

ログを出力します。

破棄したパケットのログを出力するときは、［セキュリティ設定］→［ログ通知］で［NOTICE］をチェックして下さい。

◆しない

ログを出力しません。

■DMZホスト設定

DMZホスト機能は、WAN側インターフェース（PPPoE、DHCP、固定IP）から受信したすべてのパケットのうち、LAN側への転送先が不明なものをあらかじめ設定した特定のパソコンに転送する機能です。これにより、複雑なNATの設定をしなくてもネットワークゲームを行ったり、WWWなどのサーバを外部に公開することができます。この機能は端末型接続のときのみ有効です。

●DMZホストアドレス

DMZホストにするパソコンのIPアドレスを入力します。IPアドレスを設定しない場合は、DMZホスト機能は［OFF］になります。

DMZホストの設定はLAN型接続では使用できません。

■DoS攻撃防御設定

DoS攻撃とは、正式にはDenial of Service（サービス拒否）攻撃と言います。ネットワークを通じて不正なデータを送信したり、大量にデータを送信したりすることにより、相手のサービスを使用不能にする攻撃です。
DoS攻撃防御機能により不正なアクセスを検知し、本製品およびLAN側のネットワークを保護します。

この「DoS攻撃防御設定」を「する」に設定するとすべての接続／相手先に適用されます。

■オプション

［オプション］欄にコマンドを入力して、以下の防御機能を設定することができます。入力欄をクリックするとカーソルが表示されるので、コマンドを入力して下さい。コマンドを入力する際は、以下の点に注意して下さい。

・{ }で囲まれている部分がパラメータです。パラメータの区切りには、半角スペースを入力します。
・太字は、購入時の値を意味します。
・オプション以外のパラメータを省略すると、設定できません。
・複数のコマンドを設定するときは、コマンドごとに改行して下さい。

※［オプション］欄で以下の防御機能を利用する設定を行っても、［DoS攻撃防御設定］の［DoS攻撃防御］で［する］を選択しなければ有効になりません。

●ICMPフラッディング保護機能

◆ICMPフラッディング保護機能を利用するかどうかの設定

この機能により防御できるのは、Ping Floodです。

書式　**ip dos icmpflood mode {on｜off}**
パラメータ　{on｜off}
　off：利用しない
　on：利用する

◆ICMP echo requestパケット数の設定

ICMP echo requestパケット数がこの値を超えると、フラッディングブロックタイムが経過するまで、そのIPアドレスからのICMP echo requestパケットが破棄されます。

書式　**ip dos icmpflood echo {number}**
パラメータ　{number}：ICMP echo requestパケット数（10〜50）
　購入時設定は30

●TCPインコンプリートセッション保護機能

◆TCPインコンプリートセッション保護機能を利用するかどうかの設定
この機能によりSYN Flood を防御することができます。

書式　**ip dos incomplete mode {on｜off}**
パラメータ　{on｜off}
off：利用しない
<u>on</u>：利用する

◆上限インコンプリートセッション数の設定
この値を超えるハーフオープン状態のセッションが検出されると、ポート番号に関わら ず、すべてのTCP セッションが遮断されます。

書式　**ip dos incomplete session high {session}**
パラメータ　{session}：インコンプリートセッション数の上限（1〜300）
購入時設定は300

◆下限インコンプリートセッション数の設定
TCPインコンプリートセッション保護機能によりTCP セッションが遮断された後、こ こで設定した値までハーフオープン状態のセッション数が減少したら、セッションを再開します。

書式　**ip dos incomplete session low {session}**
パラメータ　{session}：インコンプリートセッション数の下限（1〜250）
購入時設定は250

●TCP/UDP非アクティブ保護機能

◆上限非アクティブセッション数の設定
非アクティブセッション数がこの値を超えると､そのセッションは遮断されます。

書式　**ip dos inactive session high {session}**
パラメータ　{session}：非アクティブセッション数の上限（1〜250）
購入時設定は250

◆下限非アクティブセッション数の設定
非アクティブセッション保護機能によりセッションが遮断された後、ここで設定した値まで非アクティブセッション数が減少したら、セッションを再開します。

書式　**ip dos inactive session low {session}**
パラメータ　{session}：非アクティブセッション数の下限（1〜200）
購入時設定は200

●同一ホストインコンプリート、非アクティブセッション保護機能

◆同一ホストインコンプリート、非アクティブセッション保護機能を利用するかどうかの設定
この機能を利用すると、同一IPアドレスからのハーフオープン状態で非アクティブなセッションがチェックされます。
これにより、同一ホストからの下記の攻撃に対応できます。

・SYN Flood　・リロード攻撃
・Connection Flood　・UDP Flood

書式　**ip dos host incomplete mode {on｜off}**
パラメータ　{on｜off}
off：利用しない
<u>on</u>：利用する

◆インコンプリート、非アクティブセッション検出時間の設定

ここで設定した時間ごとに、インコンプリート、非アクティブセッションがチェックされます。

書式　**ip dos host incomplete time {time}**
パラメータ　{time}：インコンプリート、非アクティブセッション検出時間（50〜5000ミリ秒）
購入時設定は300ミリ秒

◆同一インコンプリート、非アクティブセッション数の設定

この値を超える、ハーフオープン状態、または非アクティブTCPセッションとUDPセッションが検出されると、そのIPアドレスからのセッションは遮断されます。その後、フラッディングブロックタイム（☞次ページ）で指定した時間を経過した時点で、そのホストとのセッションが再開されます。

書式　**ip dos host incomplete session {session}**
パラメータ　{session}：インコンプリートセッション数（1〜50）
購入時設定は10

●同一ホストフラグメンテーション保護機能

この機能を利用すると、同一IPアドレスからの断片化されたパケットがチェックされます。これにより、同一ホストからのFragment Floodに対応できます。

書式　**ip dos host fragment mode {on｜off}**
パラメータ　{on｜off}
off：利用しない
on：利用する

◆フラグメンテーション検出時間の設定

ここで設定した時間ごとに、同一IPアドレスからの断片化されたパケットがチェックされます。

書式　**ip dos host fragment time {time}**
パラメータ　{time}：フラグメンテーション検出時間（10〜60000ミリ秒）
購入時設定は10000ミリ秒

◆同一ホストフラグメンテーションパケット数の設定

この値を超える、断片化されたパケットが検出されると、そのホストからのセッションは遮断されます。その後、フラッディングブロックタイムで指定した時間を経過した時点で、そのホストとのセッションが再開されます。

書式　**ip dos host fragment packet {packet}**
パラメータ　{packet}：フラグメンテーションパケット数（1〜150）
購入時設定は30

●フラッディングブロックタイム

◆フラッディング攻撃が防御され、セッションが遮断されたとき、何秒間遮断するかを設定します。

書式　**ip dos blocktime {time}**
パラメータ　{time}：ブロックタイム（0〜30000秒）
購入時設定は300秒

設定例1　フラッディング保護機能を利用し、ICMP echo requestパケット数を40、フラッディングブロックタイムを400秒にする場合

```
ip dos icmpflood mode on
ip dos icmpflood echo 40
ip dos blocktime 400
```

設定例2　TCPインコンプリートセッション保護機能を利用し、下限セッション数を20、 上限セッション数を80にする場合

```
ip dos incomplete mode on
ip dos incomplete session low 20
ip dos incomplete session high 80
```

設定例3　TCPインコンプリートセッション保護機能を利用し、下限セッション数を20、 上限セッション数を80にする場合

```
ip dos host incomplete mode on
ip dos host incomplete session 20
ip dos host incomplete time 600
```

設定例4　同一ホストフラグメンテーション保護機能を利用し、パケット数を20、検出時間を5000にする場合

```
ip dos host fragmentation mode on
ip dos host fragmentation packet 20
ip dos host fragmentation time 5000
```

ログ通知

■基本

●ログ出力レベル

ログ出力レベルを設定します。購入時は［NOTICE］のみが設定されています。

◆DEBUG

デバッグ情報を出力します。通常は設定する必要はありません。

◆INFO

「NOTICE」よりも詳細なログ情報を出力します。

◆NOTICE

基本的なログ情報を出力します。

■ログ取得オプション

本機では以下の4つの項目についてのログ情報を取得することができます。ここでは各項目についてログ情報を取得するかどうかを設定します。

●DoS攻撃

◆出力しない

DoS攻撃に関するログ情報を取得しません。

◆出力する

DoS攻撃に関するログ情報を取得します。

●WANポート

◆出力しない

WANポートに関するログ情報を取得しません。

◆出力する

WANポートに関するログ情報を取得します。

●本体制御

◆出力しない

本体制御に関するログ情報を取得しません。

◆出力する

本体制御に関するログ情報を取得します。

●フィルタリング

◆出力しない

フィルタリングに関するログ情報を取得しません。

◆出力する

フィルタリングに関するログ情報を取得します。

IEEE802.11a

● ［設定］ボタン/［やり直し］ボタン
設定を有効にするときは、［設定］ボタンをクリックします。
設定をやり直すときは、［やり直し］ボタンをクリックします。

［設定］ボタンをクリックせずに他のページを開くと、設定した内容は消去されます。

■基本

●無線LAN使用
無線LAN機能を使用するかどうかを設定します。購入時は［する］に設定されています。

◆する
無線LAN機能を使用します。

◆しない
無線LAN機能を使用しません。

●SSID
無線グループを区別するためのIDを入力します（半角32文字まで）。なお、本製品と無線で通信する機器にも、同じIDを設定して下さい。購入時は［MN-W54］に設定されています。

セキュリティのため、SSIDはほかの無線機器と重ならないように設定して下さい。
SSIDが重なった場合、ほかの無線機器に通信の内容が流れてしまいます。
SSIDが重なったことが原因で生じたトラブルについては、弊社は一切責任を負いかねますので、あらかじめご了承下さい。

●通信チャネル
無線ネットワークで使用する通信チャネルを選択します。本製品と無線で通信する機器すべてに同じ通信チャネルを設定して下さい。購入時は［34］チャネルに設定されています。

34、38、42、46チャネルのいずれかを選択します。他の無線ネットワークと通信チャネルが重なると、通信速度が下がるなどの影響を受ける場合があります。そのときは、本製品の通信チャネルを変更して下さい。

■Super A™

米アセロス・コミュニケーションズ社の開発した、無線LANのスループットを向上させる技術です。同社の独自技術である、「パケットバースト転送」、「動的な転送最適化」、「データ圧縮機能」を組み合わせることで、実効スループットを大幅に向上しています。

接続する無線LAN 端末が、Super A™に対応している必要があります。

●Super A™の使用

Super A™を使用するかどうかを設定します。購入時は［する］に設定されています。

◆しない

Super A™機能を使用しません。

◆する

Super A™機能を使用します。

●バーストパケット数

バースト転送するパケット数（バーストパケット数）を設定することができます。2～255の間で設定できます。無線LANの環境に応じて、バーストパケット数を増減することにより、その環境に最適な設定に調整することができます。購入時は［3］に設定されています。

■セキュリティ

●無線LANステルス機能

［無線ステルスLAN機能］を［有効］にすると、SSIDを空白にしているか、または「ANY」と設定しているパソコンからの接続を許可しません。また、SSIDが検索されません。セキュリティのため、通常は［有効］にしておくことをお勧めします。購入時は［有効］に設定されています。

●認証・暗号化

本製品ではPre-Shared Key（WPA共有キー）を利用する「WPA-PSK」モードが利用できます。WPA（Wi-Fi Protected Access）セキュリティとは、Wi-Fi Allianceが提唱する認証と暗号化をあわせた最新のセキュリティ規格です。従来から利用されているWEPの弱点を克服した暗号化方式「TKIP」や、次世代の標準と言われる強力な暗号化方式「AES」を利用できるので、無線LANのセキュリティ強度を大幅に向上させることができます。購入時は［使わない］に設定されています。

◆使わない

認証、暗号化を行いません。

◆WPA-PSK

［WPA-PSK］モードで認証・暗号化を行います。

◆WEP

［WEP］モードで認証・暗号化を行います。

■WPA-PSK

［セキュリティ］で［WPA-PSK］を選択すると、次の項目が表示されます。

●WPA共有キー

［WPA共有キー］を入力します。半角英数字8～63文字の範囲内で、任意の文字列を必ず設定して下さい。外部から推測されにくいものを設定して下さい。

WPA共有キーが他の無線ネットワークと一致したことが原因で生じたトラブルについては、弊社は一切責任を負いかねますので、あらかじめご了承下さい。

●暗号化方式

TKIP/AESどちらの暗号化方式を用いるか選択します。

●キー更新時間

秒数を設定すると暗号化の鍵が変更されるため、より強固なセキュリティを確保できます。30～99999の間で設定できます。数値を小さくすると鍵の更新が頻繁に行われるため、セキュリティは強固になりますが、スループットが低下します。数値を大きくすると鍵の更新間隔が空くため、セキュリティは弱くなりますが、スループットは向上します。「0」を設定すると、暗号化の鍵は変更されません。

■WEP

［セキュリティ］で［WEP］を選択すると、次の項目が表示されます。

●WEP認証方式

オープンシステム認証/共有キー認証を設定します。☞〈P.155〉

●WEPキーの長さ

64bit、128bit、152bitのうちどのキーで行うかを設定します。

●WEPキー1/2/3/4

キーは4種類設定できます。1～4のそれぞれについて「XX:XX:XX:XX:XX」の16進数形式、もしくはASCII形式で入力します。設定できるのは64bitのうち40bitです。（64bitの場合）
本製品と無線で通信する機器すべてに、同じキーを設定して下さい。
※無線LANの対応カードによっては、パソコン側でユーティリティを使ってキーを生成することができます。詳しくは、無線LANの対応カードの説明書を参照して下さい。その場合、1～4のキーは、パソコン側で生成された順番どおりに入力して下さい。

●キーインデックス

利用するキーの番号を選択します。キーインデックスは、本製品側とパソコン側で同じである必要はありません。それぞれが設定したキーインデックスに対応するキーの内容が一致していれば通信できます。

WEPキーとキーインデックスが他の無線ネットワークと一致したことが原因で生じたトラブルについては、弊社は一切責任を負いかねますので、あらかじめご了承下さい。

IEEE802.11g/b

● ［設定］ボタン/［やり直し］ボタン
設定を有効にするときは、［設定］ボタンをクリックします。
設定をやり直すときは、［やり直し］ボタンをクリックします。

［設定］ボタンをクリックせずに他のページを開くと、設定した内容は消去されます。

■基本

●無線LAN使用
無線LAN機能を使用するかどうかを設定します。購入時は［する］に設定されています。

◆する
無線LAN機能を使用します。

◆しない
無線LAN機能を使用しません。

●SSID
無線グループを区別するためのIDを入力します（半角32文字まで）。なお、本製品と無線で通信する機器にも、同じIDを設定して下さい。購入時は［MN-W54］に設定されています。

セキュリティのため、SSIDはほかの無線機器と重ならないように設定して下さい。
SSIDが重なった場合、ほかの無線機器に通信の内容が流れてしまいます。
SSIDが重なったことが原因で生じたトラブルについては、弊社は一切責任を負いかねますので、あらかじめご了承下さい。

●通信チャネル
無線ネットワークで使用する通信チャネルを選択します。本製品と無線で通信する機器すべてに同じ通信チャネルを設定して下さい。購入時は［11］チャネルに設定されています。

◆通信チャネルの設定について
1から13チャネルのいずれかを選択します。他の無線ネットワークと通信チャネルが重なると、通信速度が下がるなどの影響を受ける場合があります。そのときは、本製品の通信チャネルを変更して下さい。

◆802.11g/bの無線LAN端末が混在する場合
802.11bの無線LAN端末と802.11gの無線LAN端末が混在する環境では、802.11gの通信速度が下がるなどの影響を受ける場合があります。

詳細設定編

■Super G™

米アセロス・コミュニケーションズ社の開発した、無線LANのスループットを向上させる技術です。同社の独自技術である、「パケットバースト転送」、「動的な転送最適化」、「データ圧縮機能」を組み合わせることで、実効スループットを大幅に向上しています。

接続する無線LAN 端末が、Super G™に対応している必要があります。

●Super G™の使用

Super G™を使用するかどうかを設定します。購入時は［する］に設定されています。

◆しない

Super G™機能を使用しません。

◆する

Super G™機能を使用します。

●バーストパケット数

バースト転送するパケット数（バーストパケット数）を設定することができます。2～255の間で設定できます。無線LANの環境に応じて、バーストパケット数を増減することにより、その環境に最適な設定に調整することができます。購入時は［3］に設定されています。

■セキュリティ

●無線LANステルス機能

［無線ステルスLAN機能］を［有効］にすると、SSIDを空白にしているか、または「ANY」と設定しているパソコンからの接続を許可しません。また、SSIDが検索されません。セキュリティのため、通常は［有効］にしておくことをお勧めします。購入時は［有効］に設定されています。

●認証・暗号化

本製品ではPre-Shared Key（WPA共有キー）を利用する「WPA-PSK」モードが利用できます。WPA（Wi-Fi Protected Access）セキュリティとは、Wi-Fi Allianceが提唱する認証と暗号化をあわせた最新のセキュリティ規格です。従来から利用されているWEPの弱点を克服した暗号化方式「TKIP」や、次世代の標準と言われる強力な暗号化方式「AES」を利用できるので、無線LANのセキュリティ強度を大幅に向上させることができます。購入時は［使わない］に設定されています。

◆使わない

認証、暗号化を行いません。

◆WPA-PSK

［WPA-PSK］モードで認証・暗号化を行います。

◆WEP

［WEP］モードで認証・暗号化を行います。

■WPA-PSK

［セキュリティ］で［WPA-PSK］を選択すると、次の項目が表示されます。［使わない］を選択している場合は表示されません。

●WPA共有キー

［WPA共有キー］を入力します。半角英数字8～63文字の範囲内で、任意の文字列を必ず設定して下さい。外部から推測されにくいものを設定して下さい。

WPA共有キーが他の無線ネットワークと一致したことが原因で生じたトラブルについては、弊社は一切責任を負いかねますので、あらかじめご了承下さい。

●暗号化方式

TKIP/AESどちらの暗号化方式を用いるか選択します。

●キー更新時間

秒数を設定すると暗号化の鍵が変更されるため、より強固なセキュリティを確保できます。30～99999の間で設定できます。数値を小さくすると鍵の更新が頻繁に行われるため、セキュリティは強固になりますが、スループットが低下します。数値を大きくすると鍵の更新間隔が空くため、セキュリティは弱くなりますが、スループットは向上します。「0」を設定すると、暗号化の鍵は変更されません。

■WEP

［セキュリティ］で［WEP］を選択すると、次の項目が表示されます。［使わない］を選択している場合は表示されません。

●WEP認証方式

オープンシステム認証/共有キー認証を設定します。☞〈P.155〉

●WEPキーの長さ

64bit、128bit、152bitのうちどのキーで行うかを設定します。

●WEPキー1/2/3/4

キーは4種類設定できます。1～4のそれぞれについて「XX:XX:XX:XX:XX」の16進数形式、もしくはASCII形式で入力します。設定できるのは64bitのうち40bitです。（64bitの場合）

本製品と無線で通信する機器すべてに、同じキーを設定して下さい。

※無線LANの対応カードによっては、パソコン側でユーティリティを使ってキーを生成することができます。詳しくは、無線LANの対応カードの説明書を参照して下さい。その場合、1～4のキーは、パソコン側で生成された順番どおりに入力して下さい。

●キーインデックス

利用するキーの番号を選択します。キーインデックスは、本製品側とパソコン側で同じである必要はありません。それぞれが設定したキーインデックスに対応するキーの内容が一致していれば通信できます。

WEPキーとキーインデックスが他の無線ネットワークと一致したことが原因で生じたトラブルについては、弊社は一切責任を負いかねますので、あらかじめご了承下さい。

MACアドレスフィルタリング

● ［設定］ボタン/［やり直し］ボタン
設定を有効にするときは、［設定］ボタンをクリックします。
設定をやり直すときは、［やり直し］ボタンをクリックします。

［設定］ボタンをクリックせずに他のページを開くと、設定した内容は消去されます。

■基本

●接続許可
無線LAN端末を、［すべて許可］または［リストの無線LAN端末のみを許可］するか選択します。購入時は［すべて許可］に設定されています。

MACアドレスは最大32件まで設定可能です。IEEE802.11aおよびIEEE802.11g/bの両方に適用されます。

● ［設定］ボタン/［やり直し］ボタン
設定を有効にするときは、［設定］ボタンをクリックします。設定をやり直すときは、［やり直し］ボタンをクリックします。

［設定］ボタンをクリックせずに他のページを開くと、設定した内容は消去されます。

■基本

●UPnP機能
UPnPをONにするかどうかを設定します。購入時は［ON］に設定されています。

◆ON
UPnP機能を有効にし、Windows Messenger、MSN Messengerの音声チャットやファイル送信などが利用できるようにします。
※LAN上のパソコンがUPnPに対応している必要があります。

◆OFF
UPnP機能を無効にします。

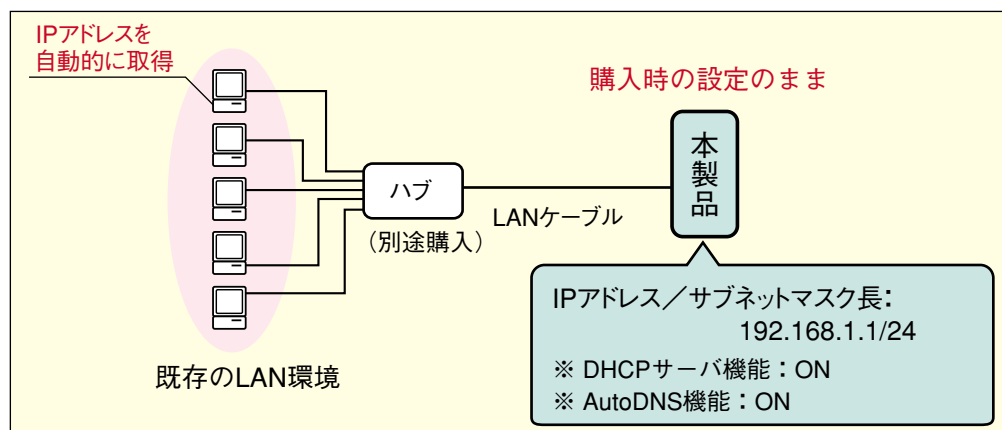
■UPnPポート 自動削除設定

●自動削除まで
UPnP対応アプリケーションを使用すると、NAT情報が登録されます。UPnP対応アプリケーションを終了したあと、ここで指定した時間が経過すると、UPnP NAT情報を自動的に削除することができます。購入時は［削除しない］に設定されています。

拡張機能編

1 既存のLAN環境で使用する

購入時のIPアドレスのまま導入する

本製品のIPアドレスを、購入時のままでLANに導入する場合について解説します。この場合、本製品の設定ページを開くには、LAN側のパソコンのIPアドレス（サブネットワークアドレス）を本製品にあわせる必要があります。

本製品の購入時の設定は次のとおりです。

本体のIPアドレス/サブネットマスク長	192.168.1.1/24
DHCPサーバ機能	ON
AutoDNS機能	ON

上記の設定のままLANで利用するには、LAN側のサブネットワークアドレスを「192.168.1.X/24」に設定し、本製品と同じサブネットワークにする必要があります。

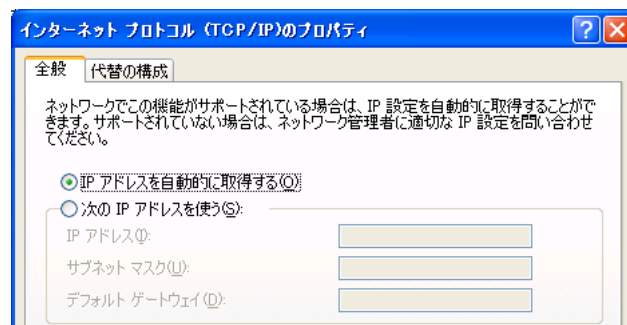
パソコン側のIPアドレスを設定する方法はいくつかありますが、ここでは、本製品のDHCPサーバ機能を使用して、本製品からIPアドレスを自動的に取得する方法を例にして解説します。

操作

■IPアドレスをDHCPサーバから自動的に取得します

1. IPアドレスを自動的に取得するように設定します。次のダイアログで設定します。

Windows XP	：	［コントロールパネル］→［ネットワークとインターネット接続］→［ネットワーク接続］→［ローカルエリア接続］のプロパティ］
Windows 2000	：	［コントロールパネル］→［ネットワークとダイヤルアップ接続］→［ローカルエリア接続］のプロパティ
Windows Me	：	［コントロールパネル］→［ネットワーク］

（例）Windows XPの場合

2. パソコンを再起動します。

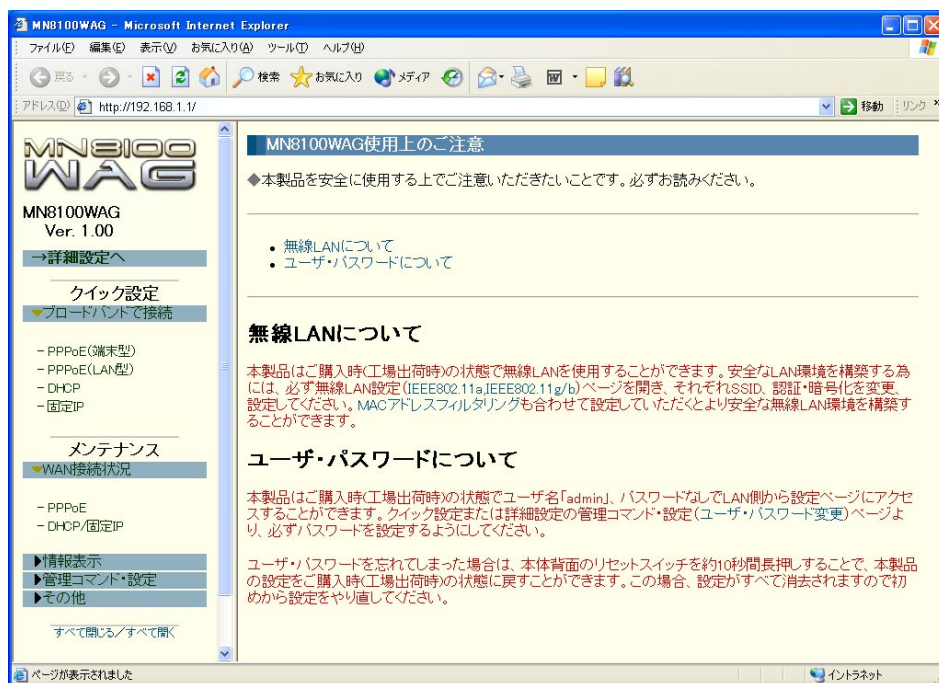
   再起動後、本製品からIPアドレスを自動的に取得できます。

この操作の前に、別のDHCPサーバからIPアドレスを取得していた場合、リース時間が経過するまで、前のIPアドレスを使用し続けます。この場合、「IPアドレスの再取得方法について」〈P.115〉を参照して、IPアドレスを更新して下さい。なお、IPアドレスを取得できるパソコンは、購入時の設定では32台までです。

拡張機能編

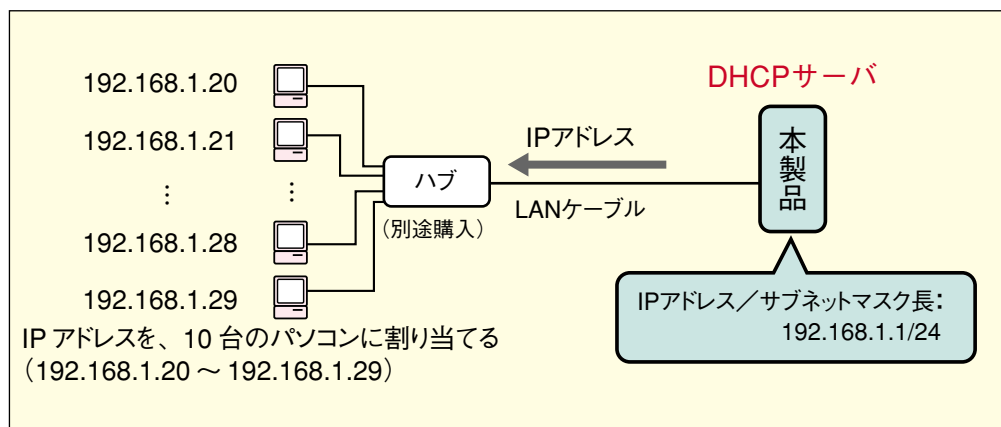
操作

■設定ページを開きます

1. WWWブラウザを起動して、［アドレス］の欄に「http://192.168.1.1/」と入力します。

以降、このページで、ルータ機能の設定を行うことができます。

拡張機能編

2 DHCPサーバ機能を使う

DHCPサーバ機能を使用するときは、設定ページでDHCPサーバ機能をONにします。

LAN内にほかのDHCPサーバがある場合は、本製品のDHCPサーバ機能をONにしないで下さい。

設定ページ

■［詳細設定］→［ルータ設定］→［LAN］

項目	設定
本体のIPアドレス/サブネットマスク長	192.168.1.1/24 ※すでに固定のIPアドレスが割り当てられたパソコンがある場合は、そのIPアドレス以外のIPアドレスを割り当てて下さい。
DHCPサーバ機能	ONを選択
開始IPアドレス/個数	192.168.1.20/10 ※割り当てるIPアドレスのうち、最初のIPアドレスと、割り当てるIPアドレスの個数を入力します。 ※すでに固定のIPアドレスが割り当てられたパソコンがある場合は、そのIPアドレス以外のIPアドレスを割り当てて下さい。

操作

■パソコンのTCP/IPの設定を変更して、IPアドレスを自動的に取得します

1. IPアドレスを自動的に取得するように設定します。次のダイアログで設定します。

   Windows XP　　：［コントロールパネル］→［ネットワークとインターネット接続］→［ネットワーク接続］→［ローカルエリア接続］のプロパティ］

   Windows 2000　：［コントロールパネル］→［ネットワークとダイヤルアップ接続］→［ローカルエリア接続］のプロパティ

   Windows Me　　：［コントロールパネル］→［ネットワーク］

2. パソコンを再起動します。

   再起動後、本製品からIPアドレスを自動的に取得できます。

この操作の前に、別のDHCPサーバからIPアドレスを取得していた場合、リース時間が経過するまで、前のIPアドレスを使用し続けます。この場合、「IPアドレスの再取得方法について」〈P.115〉を参照して、IPアドレスを更新して下さい。

◆設定されたIPアドレスを確認したいときは

DHCPサーバ機能によって自動で設定されたIPアドレスは、MS-DOSプロンプトまたはコマンドプロンプト等で確認することができます。詳しくは、「IPアドレスの再取得方法について」〈P.115〉を参照して下さい。

◆DHCPサーバ機能を使用しないときは

本製品のDHCPサーバ機能をOFFにしたときは、次の点に注意してパソコンのIPアドレスを設定し直して下さい。

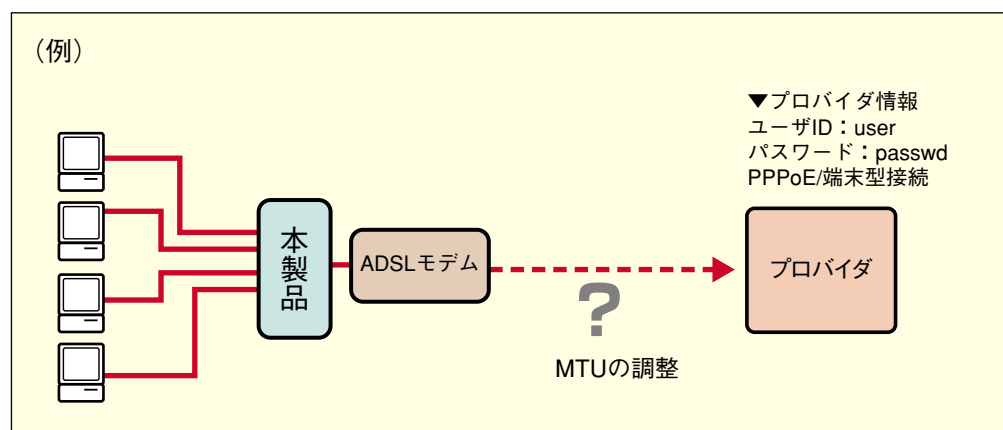
・本製品と同じサブネットのIPアドレスを設定すること
・本製品やLAN上のほかの端末（パソコンなど）のIPアドレスと重複しないように設定すること

◆IPアドレスとパソコンの組み合わせを固定にすることもできます

DHCPサーバ機能を使ってパソコンのIPアドレスを設定する際、パソコンと設定するIPアドレスの組み合わせを固定できます。「DHCPサーバ機能で割り当てるIPアドレスと、パソコンの組み合わせを固定する」〈P.122〉を参照して下さい。

ここでは、［詳細設定］メニューの［接続／相手先登録］を使って、ブロードバンドでインターネットにアクセスするための設定を詳しく解説します。

PPPoE接続する

PPPoE接続を採用しているプロバイダに接続する設定を詳しく解説します。［クイック設定］→［PPPoE（端末型）］ではうまく接続できない場合の調整方法についても解説しています。

設定ページ

1. ［詳細設定］→［接続／相手先登録］→［#0］～［#7］の中から、PPPoEを採用しているプロバイダを登録する番号をクリックします。ここでは、［#4］をクリックします。

   クリックした番号の［接続／相手先登録］画面が表示されます。

接続／相手先登録#4　Help

◆相手先の情報を登録したり、相手先に回線を手動で接続します。

Message
パラメータを入力・修正し、操作を選んで［実行］ボタンをクリックしてください。

送信パスワードは、どのような文字列を設定しても「＊」または「●」の1文字が表示されます。
変更するときは、表示されている「＊」または「●」を消去してから、新しい文字列を入力してください。

◉ 以下の情報を登録する。
○ 以下の相手先に回線を接続する。

［実行］［やり直し］

［相手先情報］	
相手先名称	
［接続］	
送信ユーザID	
送信パスワード	
DNSサーバアドレス	
接続モード	端末型接続
自動切断タイマ	150 秒
［PPPoEオプション］	

2. ［接続］の各項目で、次のように設定します。

相手先名称	名称（何でも構いません。例：プロバイダ A）を設定 ※「no」「clear」は使用できません。
送信ユーザ ID	user ※「no」「clear」は使用できません。
送信パスワード	passwd ※「no」「clear」「＊（1 文字）」「？（1 文字）」は使用できません。
DNS サーバアドレス	空白
接続モード	端末型接続
自動切断タイマ	［150］を入力

［相手先情報］

相手先名称	プロバイダA

［接続］

送信ユーザID	user
送信パスワード	●●●●●●●●●
DNSサーバアドレス	
接続モード	端末型接続
自動切断タイマ	150 秒

プロバイダからPPPoEサービス名、アクセス名の設定を指定されている場合は、［オプション］欄に、次のように入力します。

※特に指定されていない場合は、この設定は不要です。

remote {4} pppoe sname {abc}

※{ }の中には、相手先番号を入力します。

※{abc}はプロバイダから指定された名前を入力します。

［オプション］

```
remote 4 pppoe sname abc
```

3. 必要に応じて、MTUの設定を行います。

特定のWWWサイトで通信ができなかったり、ゲームなどでのデータの受信が異常に遅いときに、MTUの値を変更します。

MTU（Max Transfer Unit）とは、1回の転送で送信できるパケットの最大値を決める値のことです。MTUサイズが大きいほど一度に多くのデータを送れますが、MTUサイズを大きくしてしまうと、例えば、通信品質があまり良くなくパケットの損失が発生してしまうような回線では、再送の発生により転送効率が悪くなりかえって通信速度が遅くなるという結果になることがあります。「1454」などの値を入力して下さい。

※問題なく動作している場合は、MTUの設定を行う必要はありません。設定を行わない場合、PPPoE接続では「1454」が使用されます（PPPoE以外の接続では1500が使用されます）。

[MTU設定]	
MTUサイズ	1454

4. [以下（以上）の情報を登録する。] を選択し、[実行] ボタンをクリックします。

プロバイダに関する設定が終了しました。
実際にプロバイダに接続するには、どれか1台のパソコンで接続の操作を行うと、どのパソコンでもインターネットにアクセスできます。

5. WAN側からの不正なアクセスを防止するため、設定ページにユーザIDとパスワードを設定します。[メンテナンス] の [管理コマンド・設定] → [ユーザ・パスワード変更] をクリックします。

[管理コマンド・設定（ユーザ・パスワード変更）] 画面が表示されます。

管理コマンド・設定(ユーザ・パスワード変更) Help

◆ユーザID・パスワードを変更します。

Message

パラメータを入力・修正して [設定] ボタンをクリックしてください。

パスワードは、どのような文字列を設定しても「＊」または「●」の1文字が表示されます。
変更するときは、表示されている「＊」または「●」を消去してから、新しい文字列を入力してください。

設定　やり直し

[ユーザ・パスワード変更]	
ユーザID	admin
パスワード	
パスワード(再入力)	

6. 次のように入力します。

ユーザID	ユーザIDを入力 ※「no」「clear」は使用できません。
パスワード	パスワードを入力 ※「no」「clear」「＊（1文字）」「？（1文字）」は使用できません。
パスワード（再入力）	[パスワード] に入力した文字を入力

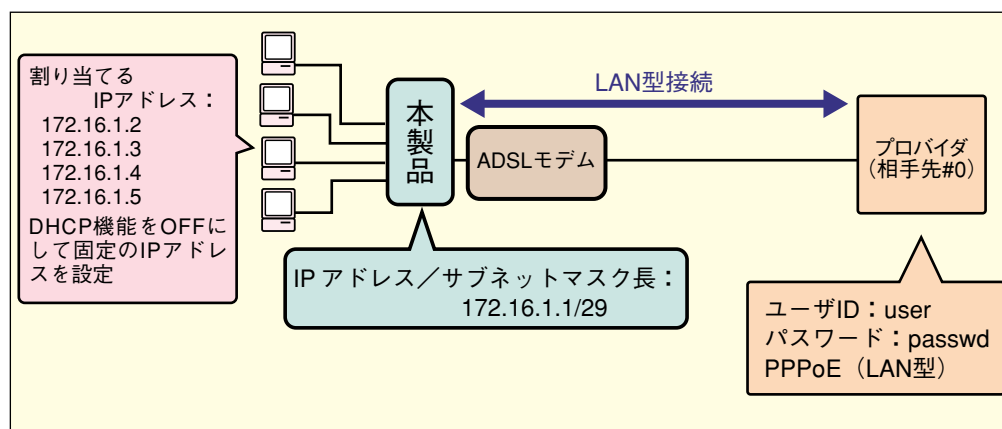
拡張機能編

7. ［設定］ボタンをクリックします。

以降、管理者が設定ページを開くときは［パスワード要求］ダイアログで上記で設定した［ユーザID］と［パスワード］を入力して下さい。ユーザIDとパスワードを忘れると、設定ページを開くことができません。ご注意下さい。

ADSLまたはFTTHを使用してインターネットに常時接続できる環境では、外部からの不正アクセスや攻撃の被害に遭う危険性も高くなります。本製品のステルスモード、SPI機能、IPフィルタなどを使用して、セキュリティ対策は十分に行って下さい。なお、クイック設定を行ったときは、自動的にIPフィルタが設定されます。
ステルスモード、SPI機能、IPフィルタに関しては、それぞれP.148〜152を参照して下さい。

PPPoE（IPアドレス払い出し）LAN型接続する

本製品のLANポートに接続したパソコン（またはハブを経由したパソコン）から、プロバイダにLAN型接続する場合の設定例を紹介します。

プロバイダとLAN型接続の契約をする必要があります。

設定ページ

■ ［詳細設定］→［接続／相手先登録］→［#0］

相手先名称	名称（何でも構いません）を設定
送信ユーザ ID	user
送信パスワード	passwd
接続モード	［LAN 型接続］を選択

■［詳細設定］→［ルータ設定］→［LAN］

本体の IP アドレス / サブネットマスク長	172.16.1.1/29
DHCP サーバ機能	OFF

設定ページ

■手動接続します

1. ［詳細設定］→［接続／相手先登録］で、接続したい相手先登録番号（例では#0）をクリックします。

2. ［以下（以上）の相手先に回線を接続する。］をクリックし、［実行］ボタンをクリックします。

4 NAT機能を使う

パソコン3台のうち、特定の1台だけでインターネットに接続する（端末型）

LAN上のパソコンのうち、特定のIPアドレスのパソコンだけでインターネットに接続するには、「IPアドレス変換（NAT）テーブル」を設定する必要があります。なお、それ以外のパソコンはインターネットに接続できません。

設定ページ

■［詳細設定］→［接続／相手先登録］→［#0］

相手先名称	名称（何でも構いません）を設定
送信ユーザID	user
送信パスワード	passwd
接続モード	［端末型接続］を選択

■［詳細設定］→［ルータ設定］→［LAN］

本体のIPアドレス/ サブネットマスク長	192.168.1.1/24
DHCPサーバ機能	OFF
オプション	ip nat 1 192.168.1.1-192.168.1.2/*/* ipcp ※ 192.168.1.1 が含まれないと、AutoDNS 機能が使用できません。 ※「ipcp」を設定すると、プライベート IP アドレスと、PPPoE（端末型）での接続に割り当てられる IP アドレスの変換になります。

操作

■パソコンのTCP/IPの設定を変更して、固定のIPアドレスを割り当てます

1. LAN上のパソコンにすべて、プライベートIPアドレスを割り当てます。次のダイアログで設定します。

Windows XP	：［コントロールパネル］→［ネットワークとインターネット接続］→［ネットワーク接続］→［ローカルエリア接続］のプロパティ］
Windows 2000	：［コントロールパネル］→［ネットワークとダイヤルアップ接続］→［ローカルエリア接続］のプロパティ
Windows Me	：［コントロールパネル］→［ネットワーク］

2. パソコンを再起動します。

拡張機能編

パソコン10台のうち、特定の5台だけで インターネットに接続する（端末型）

LAN上のパソコンのうち、特定のIPアドレスのパソコンだけインターネットに接続させるには、「IPアドレス変換（NAT）テーブル」を設定します。さらに、DHCPサーバ機能で、本製品から特定のパソコンに、常に特定のIPアドレスを割り当てます。

設定ページ

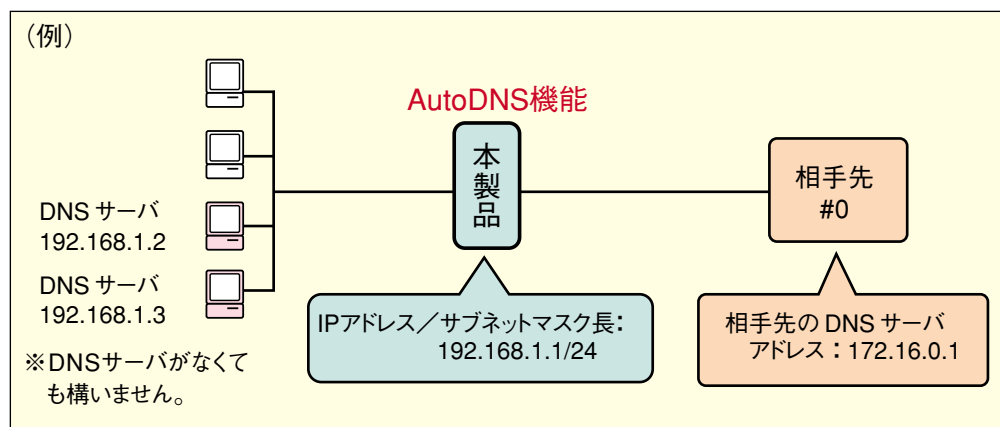
■［詳細設定］→［接続／相手先登録］→［#0］

相手先名称	名称（何でも構いません）を設定
送信ユーザ ID	user
送信パスワード	passwd
接続モード	［端末型接続］を選択

■［詳細設定］→［ルータ設定］→［LAN］

本体のIPアドレス/ サブネットマスク長	192.168.1.1/24
DHCP サーバ機能	ON
開始 IP アドレス / 個数	192.168.1.2/10
オプション	ip nat 1 192.168.1.1-192.168.1.6 ipcp ip host 192.168.1.2 user1.tmp.co.jp 0a:1b:2c:00:11:22 ip host 192.168.1.3 user2.tmp.co.jp 0a:1b:2c:00:11:23 ip host 192.168.1.4 user3.tmp.co.jp 0a:1b:2c:00:11:24 ip host 192.168.1.5 user4.tmp.co.jp 0a:1b:2c:00:11:25 ip host 192.168.1.6 user5.tmp.co.jp 0a:1b:2c:00:11:26 （user5.tmp.co.jp：任意のホスト名を割り当てます。 0a:1b:2c:00:11:26：パソコンのMACアドレスです。） ※同じパソコンに同じIPアドレスが割り当てられるようにします。

5 AutoDNS機能を使う

本製品のAutoDNS機能を使用すると、接続する相手先を変更したときでも、パソコンのDNSサーバのIPアドレスを設定し直す必要がなくなります。なお、購入時はAutoDNS機能はONです。

設定ページ

■ ［詳細設定］ → ［接続／相手先登録］ → ［#0］

DNS サーバアドレス	172.16.0.1

■ ［詳細設定］ → ［ルータ設定］ → ［LAN］

本体のIPアドレス/サブネットマスク長	192.168.1.1/24
AutoDNS機能	ONを選択
LAN 側 DNS サーバアドレス（プライマリ）/LAN 側 DNS サーバアドレス（セカンダリ）	LAN 側の DNS サーバを常に優先して使いたいとき、これらの項目にその DNS サーバの IP アドレスを入力します。 192.168.1.2 192.168.1.3 ※ LAN 側に DNS サーバがなくても本機能が使えます。LAN 側に DNS サーバがないときは、空白にして下さい。

操作

■パソコンのTCP/IPの設定を変更します

各OSのTCP/IP設定の画面で、次のように設定します。

●Windows XPの場合

［コントロールパネル］→［ネットワークとインターネット接続］→［ネットワーク接続］→［ローカルエリア接続］のプロパティで設定します。

本製品の DHCP サーバ機能が ON のとき	
［全般］タブ	［DNS サーバーのアドレスを自動的に取得する］を選択
本製品の DHCP サーバ機能が OFF のとき	
［全般］タブ	［次の DNS サーバーのアドレスを使う］を選択し、次の項目を設定 ［優先 DNS サーバー］→本製品の IP アドレスを入力

●Windows 2000の場合

［コントロールパネル］→［ネットワーク接続］→［ローカルエリア接続］のプロパティで設定します。

本製品の DHCP サーバ機能が ON のとき	
［全般］タブ	［DNS サーバーのアドレスを自動的に取得する］を選択
本製品の DHCP サーバ機能が OFF のとき	
［全般］タブ	［次の DNS サーバーのアドレスを使う］を選択し、次の項目を設定 ［優先 DNS サーバー］→本製品の IP アドレスを入力

●Windows Meの場合

［コントロールパネル］→［ネットワーク］で設定します。

本製品の DHCP サーバ機能が ON のとき	
［DNS 設定］タブ	［DNS を使わない］を選択
［ゲートウェイ］タブ	［インストールされているゲートウェイ］からすべての IP アドレスを削除
本製品の DHCP サーバ機能が OFF のとき	
［DNS 設定］タブ	［DNS を使う］を選択し、次の項目を設定 ホスト → パソコンに付ける名前を入力 DNS サーバの検索順 → 本製品の IP アドレスを入力
［ゲートウェイ］タブ	本製品または同一サブネット上のゲートウェイ（ルータ）の IP アドレスを入力

この操作を行っても通信できないときは、下記の「AutoDNS機能を使用しないときは」に従って操作して下さい。

◆AutoDNS機能を使用しないときは

本製品のAutoDNS機能をOFFにしたときは、パソコンのTCP/IPを次のように設定します。

・Windows XPの場合

［コントロールパネル］→［ネットワークとインターネット接続］→［ネットワーク接続］→［ローカルエリア接続］のプロパティで設定します。

本製品のDHCPサーバ機能がON、かつ、LAN側DNSサーバアドレスを設定しているとき	
［全般］タブ	［DNSサーバのアドレスを自動的に取得する］を選択
上記以外のとき	
［全般］タブ	［次のDNSサーバーのアドレスを使う］を選択し、次の項目を設定 ［優先DNSサーバー］［代替DNSサーバー］ →使用するDNSサーバのIPアドレスを入力

・Windows 2000の場合

［コントロールパネル］→［ネットワーク接続］→［ローカルエリア接続］のプロパティで設定します。

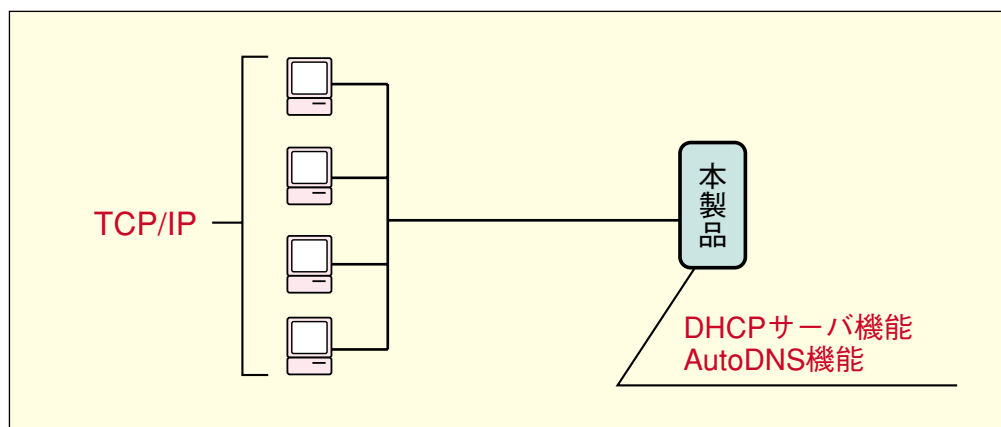
本製品のDHCPサーバ機能がON、かつ、LAN側DNSサーバアドレスを設定しているとき	
［全般］タブ	［DNSサーバのアドレスを自動的に取得する］を選択
上記以外のとき	
［全般］タブ	［次のDNSサーバーのアドレスを使う］を選択し、次の項目を設定 ［優先DNSサーバー］［代替DNSサーバー］ →使用するDNSサーバのIPアドレスを入力

・Windows Meの場合

［コントロールパネル］→［ネットワーク］で設定します。

本製品のDHCPサーバ機能がON、かつ、LAN側DNSサーバアドレスを設定しているとき	
［全般］タブ	［DNSサーバのアドレスを自動的に取得する］を選択
上記以外のとき	
［全般］タブ	［次のDNSサーバーのアドレスを使う］を選択し、次の項目を設定 ［優先DNSサーバー］［代替DNSサーバー］ →使用するDNSサーバのIPアドレスを入力

6 IPアドレスの再取得方法について

一度DHCPサーバからIPアドレスを取得した場合、IPアドレスを変更しても、IPアドレスのリース期間が経過するまでは自動的に更新されません。更新するための操作方法について解説します。

操作

■Windows XPの場合

1. ［スタート］ボタン→［コントロールパネル］を選択します。

2. ［ネットワークとインターネット接続］→［ネットワーク接続］を選択します。次に［ローカルエリア接続］を右クリックし、［状態］を選択します。
   ［ローカルエリアネットワークの状態］ダイアログが表示されます。

3. ［サポート］タブをクリックし、［修復］ボタンをクリックします。
   以前取得したIPアドレスが無効になり、新しいIPアドレスが設定されます。

■Windows 2000の場合

1. ［スタート］ボタン→［プログラム］→［アクセサリ］→［コマンドプロンプト］をクリックします。
   ［コマンドプロンプト］ウィンドウが表示されます。

2. 「ipconfig/release」と入力し、［Enter］キーを押します。
   以前取得したIPアドレスは無効になります。

3. 「ipconfig/renew」と入力し、［Enter］キーを押します。
   新しいIPアドレスが設定されます。

■Windows Meの場合

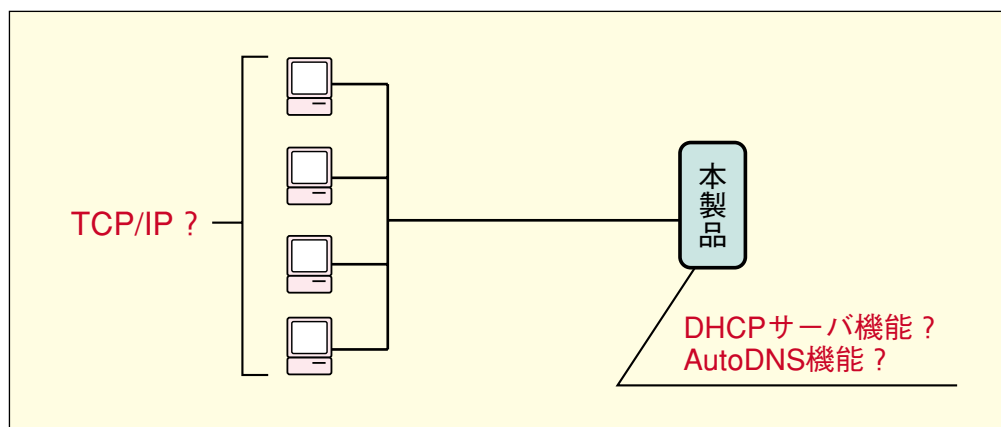
1. ［スタート］ボタン→［プログラム］→［MS-DOSプロンプト］をクリックします。
   ［MS-DOSプロンプト］ウィンドウが表示されます。

2. 「winipcfg」と入力し、［Enter］キーを押します。
   ［IP設定］ダイアログが表示されます。

3. 使用しているEthernetボードを選択し、［解放］ボタンをクリックします。
   ［IPアドレス］が「0.0.0.0」に変わり、以前取得したIPアドレスは無効になります。

4. ［書き換え］ボタンをクリックします。
   新しいIPアドレスが設定されます。

7 TCP/IP設定早見表

本製品のDHCPサーバ機能とAutoDNS機能の設定に対する、パソコンのTCP/IPの設定内容をまとめると、次のようになります。

操作

■Windows XPの場合

		AutoDNS 機能	
		ON	OFF
DHCPサーバ機能	ON	●IP アドレス ［IP アドレスを自動的に取得する］を選択 ●DNS ［DNS サーバーのアドレスを自動的に取得する］を選択	●IP アドレス ［IP アドレスを自動的に取得する］を選択 ●DNS ［DNS サーバーのアドレスを自動的に取得する］を選択 ☞「DNS の設定について」〈P.119〉を参照
	OFF	●IP アドレス ［次の IP アドレスを使う］を選択し、IP アドレス・サブネットマスクを入力、［デフォルトゲートウェイ］に本製品の IP アドレスを入力 ●DNS ［次の DNS サーバーのアドレスを使う］を選択し、［優先 DNS サーバー］に、本製品の IP アドレスを入力	●IP アドレス ［次の IP アドレスを使う］を選択し、IP アドレス・サブネットマスクを入力、［デフォルトゲートウェイ］に本製品の IP アドレスを入力 ●DNS ［次の DNS サーバーのアドレスを使う］を選択し、［優先 DNS サーバー］に、使用する DNS サーバの IP アドレスを入力

■Windows 2000の場合

		AutoDNS 機能	
		ON	OFF
DHCPサーバ機能	ON	●IP アドレス ［IP アドレスを自動的に取得する］を選択 ●DNS ［DNS サーバーのアドレスを自動的に取得する］を選択	●IP アドレス ［IP アドレスを自動的に取得する］を選択 ●DNS ［DNS サーバーのアドレスを自動的に取得する］を選択 ☞「DNS の設定について」〈P.119〉を参照
	OFF	●IP アドレス ［次の IP アドレスを使う］を選択し、IP アドレス・サブネットマスクを入力、［デフォルトゲートウェイ］に本製品の IP アドレスを入力 ●DNS ［次の DNS サーバーのアドレスを使う］を選択し、［優先 DNS サーバー］に、本製品の IP アドレスを入力	●IP アドレス ［次の IP アドレスを使う］を選択し、IP アドレス・サブネットマスクを入力、［デフォルトゲートウェイ］に本製品の IP アドレスを入力 ●DNS ［次の DNS サーバーのアドレスを使う］を選択し、［優先 DNS サーバー］に、使用する DNS サーバの IP アドレスを入力

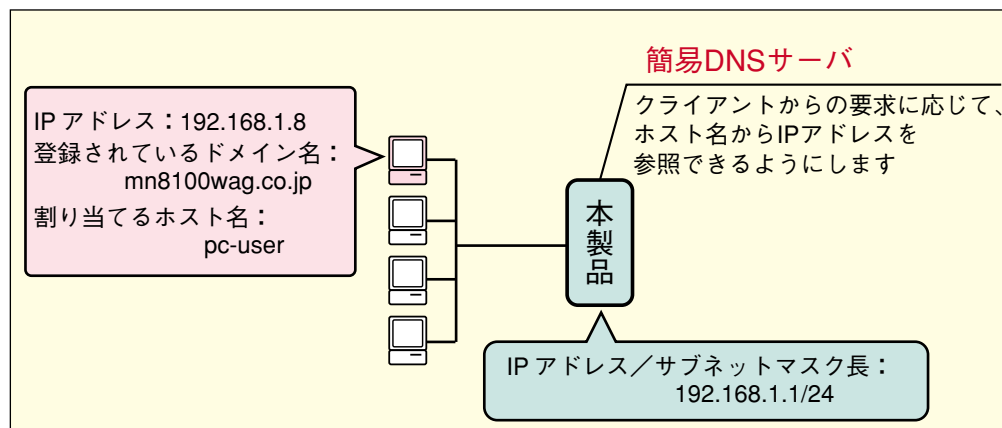
■Windows Meの場合

		AutoDNS 機能	
		ON	OFF
DHCPサーバ機能	ON	●IP アドレス ［IPアドレスを自動的に取得］を選択 ●DNS 設定 ［DNS を使わない］を選択	●IP アドレス ［IP アドレスを自動的に取得］を選択 ●DNS 設定 ［DNS を使わない］を選択 ☞「DNS の設定について」〈P.119〉を参照
	OFF	●IP アドレス ［IP アドレスを指定］を選択し、IP アドレス、サブネットマスクを入力 ●DNS 設定 ［DNS を使う］を選択し、［ホスト］にパソコンに付ける名前を、［ドメイン名］に使用するドメイン名を、［DNS サーバの検索順］に本製品の IP アドレスを入力 ●ゲートウェイ 本製品または同一ネット上のゲートウェイ（ルータ）の IP アドレスを入力	●IP アドレス ［IP アドレスを指定］を選択（IP アドレス・サブネットマスクを入力） ●DNS 設定 ［DNS を使う］を選択し、［ホスト］にパソコンに付ける名前を、［ドメイン名］に使用するドメイン名を、［DNS サーバの検索順］に使用する DNS サーバの IP アドレスを入力 ●ゲートウェイ 本製品または同一ネット上のゲートウェイ（ルータ）の IP アドレスを入力

拡張機能編

◆DNSの設定について
［詳細設定］→［ルータ設定］→［LAN］画面で［LAN側DNSサーバアドレス（プライマリ）］を設定していると、その設定内容がIPアドレスとともに本製品からパソコンに通知されます（DHCPサーバ機能による）。
［LAN側DNSサーバアドレス（プライマリ）］［LAN側DNSサーバアドレス（セカンダリ）］をともに設定していないときは、［DHCPサーバ機能］がOFF、［AutoDNS機能］がONの場合と同様に、各パソコンでDNSサーバのIPアドレスを設定して下さい。

8 簡易DNSサーバにする

AutoDNS機能を使うとき、本製品を簡易DNSサーバとして使用できます。簡易DNSサーバは、ドメイン名からIPアドレスを検索するドメイン名解決要求と、IPアドレスからドメイン名を検索するドメイン名逆引き要求に応じます（UDP/53による）。

設定ページ

簡易DNSサーバ機能を使用するには、パソコンのホスト名と対応するIPアドレスの組み合わせを本製品側に登録しておく必要があります。組み合わせは、ホスト情報として最大32個まで登録できます。
頻繁に接続するパソコンは、ホスト情報に登録することをお勧めします。

■［詳細設定］→［ルータ設定］→［LAN］

本体のIPアドレス/サブネットマスク長	192.168.1.1/24
AutoDNS機能	［ON］を選択
オプション	ip host 192.168.1.8 pc-user.mn8100wag.co.jp ※この場合、「pc-user.mn8100wag.co.jp」または「pc-user」のドメイン名解決要求に応じます。

拡張機能編

操作

■DHCPサーバ機能がONのとき

パソコン側での設定は不要です。

■DHCPサーバ機能がOFFのとき

パソコン側のDNSサーバの設定で、本製品のIPアドレスを指定する必要があります。

●Windows XPの場合

［コントロールパネル］→［ネットワークとインターネット接続］→［ネットワーク接続］→［ローカルエリア接続］のプロパティで、［次のDNSサーバーのアドレスを使う］を選択し、「192.168.1.1」を指定します。

●Windows 2000の場合

［コントロールパネル］→［ネットワークとダイヤルアップ設定］→［ローカルエリア接続］のプロパティで、［次のDNSサーバーのアドレスを使う］を選択し、「192.168.1.1」を指定します。

●Windows Meの場合

［コントロールパネル］→［ネットワーク］→［TCP/IP］のプロパティ→［DNS設定］タブ→［DNSサーバ検索順］に、「192.168.1.1」を指定します。

◆簡易DNSサーバの動作について

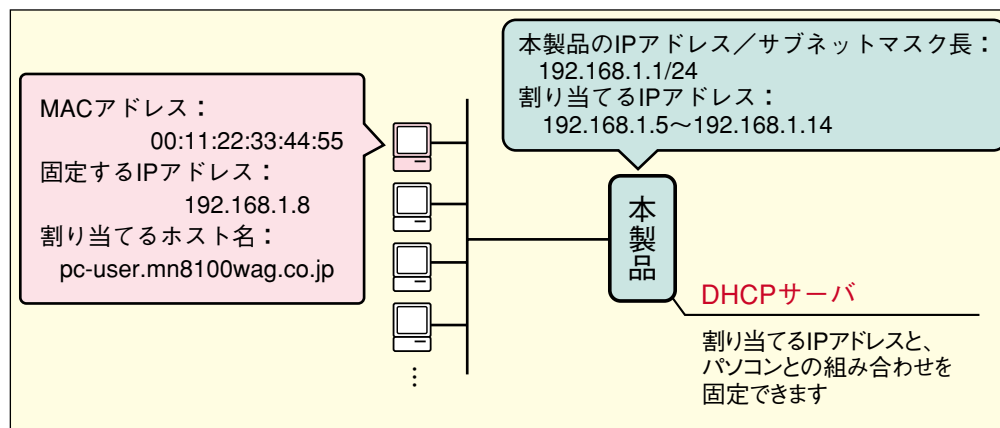
・ドメイン名解決要求を受信したとき
簡易DNSサーバはホスト情報を検索します。一致する情報がある場合、対応するIPアドレスをパソコンに送信します。一致する情報がない場合、通常のAutoDNS機能の動作に従います。
このとき、自動接続の設定をしていると、自動的に接続されるので注意が必要です。
また、LAN側だけでなく、WAN側からのドメイン名解決要求にも応じます。

・ドメイン名逆引き要求を受信したとき
簡易DNSサーバはホスト情報を検索します。一致する情報がある場合、最初に登録されているホスト名をパソコンに送信します。

なお、ホスト情報は、DHCPサーバ機能で割り当てるIPアドレスとパソコンの組み合わせを固定する場合にも使われます。「DHCPサーバ機能で割り当てるIPアドレスと、パソコンの組み合わせを固定する」〈P.122〉を参照して下さい。

拡張機能編

9 DHCPサーバ機能で割り当てるIPアドレスと、パソコンの組み合わせを固定する

本製品のDHCPサーバ機能を使ってパソコンのIPアドレスを設定する際、パソコンと設定するIPアドレスの組み合わせを固定できます。設定するIPアドレスとパソコンの組み合わせは、ホスト情報として最大32個まで登録できます。

ホスト情報は、本製品を簡易DNSサーバにする場合にも使われます。簡易DNSサーバについては、「簡易DNSサーバにする」〈P.120〉を参照して下さい。

設定ページ

■［詳細設定］→［ルータ設定］→［LAN］

本体のIPアドレス/サブネットマスク長	192.168.1.1/24
DHCPサーバ機能	［ON］を選択
開始IPアドレス/個数	192.168.1.5/10
オプション	ip host 192.168.1.8 pc-user.mn8100wag.co.jp 00:11:22:33:44:55 ※「192.168.1.8」は必ず「00:11:22:33:44:55」のパソコンに割り当てられますが、 192.168.1.5〜192.168.1.7 192.168.1.9〜192.168.1.14 は不特定のパソコンに割り当てられます。

DHCPサーバ機能で割り当てるIPアドレスとパソコンの組み合わせを固定する場合は、必ずホスト情報にMACアドレスを登録して下さい。

◆本製品を簡易DNSサーバにしているとき

本製品を簡易DNSサーバとするために設定したホスト情報（MACアドレスの登録がないホスト情報）を登録した場合も、指定したIPアドレスが［ルータ設定（LAN）］画面の［開始IPアドレス/個数］に該当すると、DHCPサーバ機能が働き、パソコンにIPアドレスが割り当てられます。

例）　ip host 192.168.1.9 pc-user.mn8100wag.co.jp

DHCPサーバ機能を使ってIPアドレスを設定する不特定のパソコンに、IPアドレス「192.168.1.9」が割り当てられます。

また、IPアドレス「192.168.1.9」のドメイン名逆引き要求には、「pc-user.mn8100wag.co.jp」と応じます。

◆パソコンのMACアドレスを確認する

パソコンのMACアドレスを確認するには、次の方法で行います。

・Windows XPの場合

1.［スタート］メニュー→［コントロールパネル］→［ネットワークとインターネット接続］→［ネットワーク接続］の順に選択します。
2.［ローカルエリア接続］を右クリックし、［状態］を選択します。
［ローカルエリア接続の状態］が表示されます。
3.［サポート］タブをクリックし、［詳細］ボタンをクリックします。
［ネットワーク接続の詳細］ダイアログが表示され、［物理アドレス］にMACアドレスが表示されます。

・Windows 2000の場合

1.［スタート］メニュー→［アクセサリ］→［コマンドプロンプト］の順に選択します。
2.「ipconfig/all¦more」と入力して［Enter］キーを押します。
3.「Physical Address」に、MACアドレスが表示されます。

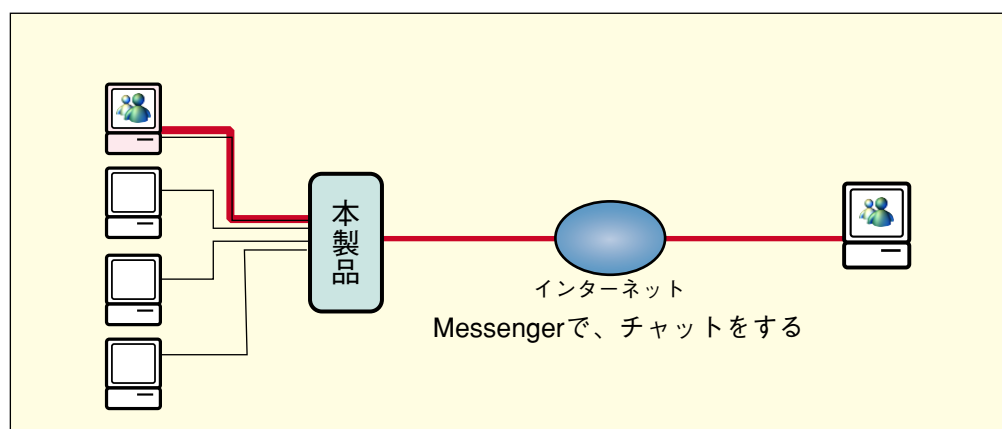
・Windows Meの場合

1.［スタート］メニュー→［プログラム］→［MS-DOSプロンプト］の順に選択します。
2.「C:>」の後ろに「winipcfg」と入力します。
［IP設定］が開きます。
3. ポップアップメニューから、使用しているEthernetアダプタ名を選択します。
［アダプタアドレス］にMACアドレスが表示されます。

10 Messengerを使う

ここでは、音声・ビデオチャットの代表的なソフトウェアの、Windows Messenger、MSN Messengerを本製品で使うときに必要な設定を解説します。

Windows Messenger、MSN Messengerを使う

LANポートにつないだパソコンと、本製品のUPnP（Universal Plug and Play：ユニバーサルプラグアンドプレイ）機能を利用すると、Windows Messenger4.7以上、またはMSN Messenger6.1以上を複数台のパソコンで利用できます。本製品は購入時にUPnP機能がONになっているので、とくに設定をする必要がありません。

◆Messengerを同時に利用できるパソコンは、4台までです。

◆UPnPを利用できるパソコンは、Windows XPおよびWindows Meです。
Windows Meの場合は、［コントロールパネル］→［アプリケーションの追加と削除］で［ユニバーサルプラグアンドプレイ］をインストールして下さい。

◆音声チャットを行うには、マイク・スピーカー、またはヘッドセットが別途必要です。

◆ビデオチャットを行うには、マイク・スピーカー（またはヘッドセット）、カメラ（USBカメラ）などが別途必要です。

拡張機能編

■利用できる機能

本製品で利用できるWindows Messenger、またはMSN Messengerの機能は次のとおりです。

OS	Windows XP		Windows Me
Messenger のバージョン	Windows Messenger 4.7, 5.0	MSN Messenger 6.1	MSN Messenger 6.1
インスタントメッセージ	○	○	○
音声チャット	○	○	○※
ビデオチャット	○	○	○※
ファイル転送	×	○※	○※
アプリケーション共有	○	○	−
ホワイトボード	○	○	−
リモートアシスタンス	○	○	−
同一 LAN 内同士の音声チャット	○	○	○※
同一 LAN 内同士のファイル送信	○	○	○※
同一 LAN 内同士のビデオチャット	○	○	○※
同一 LAN 内同士のアプリケーション共有	○	○	−
同一 LAN 内同士のホワイトボード	○	○	−

※は、UPnP準拠の機能ではありませんが、本製品独自の機能によって利用できます。

◆Windows XPをご利用の場合は、[Windows Update] から [Service Pack1] と [重要な更新] のすべてをインストールして下さい。

◆Windows Meをご利用の場合は、DirectX8.1以降をインストールして下さい。また、[Windows Update] から [Service Pack1] と [重要な更新] のすべてをインストールして下さい。

Windows Messenger / MSN Messengerがうまく動作しないときは、「困ったときは」の「Windows Messenger / MSN Messengerで通信できない」〈P.187〉をお読み下さい。

拡張機能編

設定ページ

■UPnPポートの自動削除の時間を設定する

MessengerなどUPnP対応の機能を使用することにより、一定時間通信がないとき動的に開いた本製品のポートを自動的に削除することができます。セキュリティ対策のため、自動削除までの時間を設定しておくことをお勧めします。機能によっては通信が開始したときしか使用しないポートがあるため、通信開始から設定時間が経過した際にポートが削除されることがあります。その場合は、次回の通信ができなくなるので、Messengerなどを一度終了し、再度起動して下さい。

※自動削除までの時間を設定しないときは、Messengerなどからの削除要求か、Messengerで登録した有効期間が過ぎるまでは、ポートは開いたままになります。

1. ［詳細設定］→［UPnP設定］をクリックします。

［UPnP設定］画面が表示されます。

2. ［自動削除まで］の項目で、開いたポートを削除するまでの時間を設定します。

1時間～24時間まで1時間毎に設定できます。なお、［削除しない］を選択すると、自動削除は行われません。

※24時間以上断続的にMessengerを利用するときは、［削除しない］を選択して下さい。この場合、ポートを削除するときは、本製品を再起動して下さい。

3. ［設定］ボタンをクリックします。

以降、登録したポートを使用するMessengerを利用しなくなってから設定した時間が経過すると、ポートが削除されます。

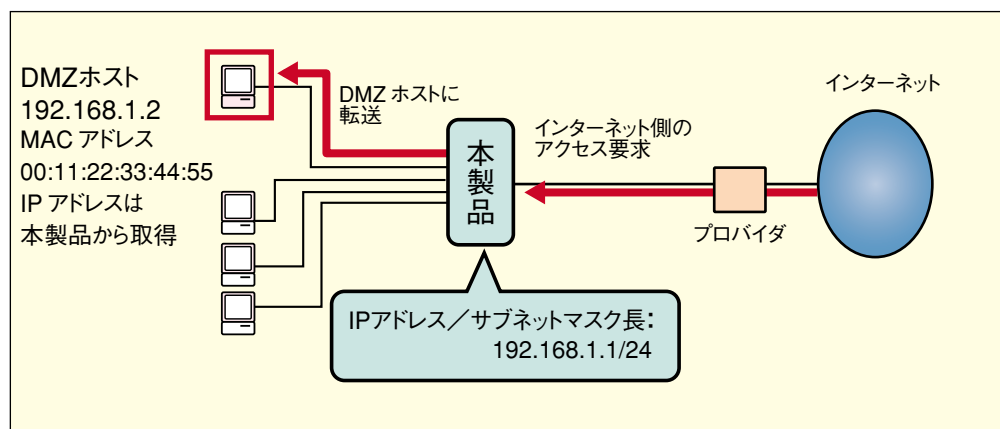
拡張機能編

タイマの設定でポートが削除されたあと、そのポートを使用するMessengerを再度ご利用になる場合は、パソコン側でMessengerをいったん終了してから、再起動して下さい。

◆UPnPの状況を確認する
［詳細設定（またはクイック設定）］→［情報表示］→［UPnP状況］をクリックすると、Messengerが本製品に対して要求したポートマッピングの状況を確認できます。電源を入れ直すと、ポートマッピングの情報は削除されます。

◆UPnP機能を使用しないとき
UPnP機能を使わないときは、［UPnP設定］画面の［UPnP機能］を［OFF］にします。

11 DMZホストを設定する

DMZホスト機能を設定すると、IPアドレス（変換）テーブルで変換できない、インターネット側から発信された宛先不明のパケットを、特定のパソコンに転送できます。使用ポートが特定できないネットワークゲームなどのアプリケーションを利用するときや、外部にサーバを公開するときなどに設定すると便利です。

◆DMZホスト機能は、端末型でインターネットに接続しているときのみ有効です。

◆DMZホストになったパソコンは、インターネット側からの攻撃を受けやすくなるので注意して下さい。

設定ページ

■［詳細設定］→［セキュリティ設定］→［ルータ］

DMZ ホストアドレス	192.168.1.2

■［詳細設定］→［ルータ設定］→［LAN］

オプション	ip host 192.168.1.2 dhost.mn8100wag.co.jp 00:11:22:33:44:55 （dhost.mn8100wag.co.jp：任意のホスト名を割り当てます。） （00:11:22:33:44:55：パソコンのMACアドレスです。）

拡張機能編

DMZホストを登録した場合、クイック設定をしたときに自動的に追加されるフィルタによって、外部からTCPによる通信ができない場合があります。その場合は、tcpestを禁止するフィルタを削除するか、またはtcpを通過させるフィルタを追加して下さい。

※クイック設定で自動的に追加されるフィルタについては、「クイック設定で自動的に設定されるフィルタ」〈P.190〉を参照して下さい。

・tcpを追加させるフィルタの設定例
接続相手先 → #0
DMZホストのIPアドレス → 192.168.1.2

```
ip filter 10 pass in * 192.168.1.2/32 tcpest * * remote 0
ip filter 11 pass in * 192.168.1.2/32 tcp * * remote 0
```

※フィルタ番号の「10」「11」は一例です。設定環境に合わせて番号を書き換えて下さい。

上記2つのフィルタを追加します。

12 不正なアクセスを検知し、防御する（DoS攻撃防御）

DoS攻撃とは、正式にはDenial of Service（サービス拒否）攻撃と言います。ネットワークを通じて不正なデータを送信したり、大量にデータを送信したりすることにより、相手のサービスを使用不能にする攻撃です。
本製品では、DoS攻撃防御機能により不正なアクセスを検知し、本製品およびLAN側のネットワークを保護します。
導入時の設定では、DoS攻撃防御機能はオフになっています。

◆プライベートアドレスのネットワークを接続する場合
DoS攻撃防御をオンにすると、IP Spoofing攻撃（☞次ページ参照）防御の機能がオンになり、送信元のIPアドレスがプライベートアドレスの場合、そのパケットが破棄されます。そのため、以下のような通信ができなくなる場合があります。
・2拠点のプライベートアドレスネットワークをLAN型で接続する場合
・本製品のLAN側で使用しているIPアドレスがプライベートアドレスで、リモートアクセスを受ける場合
　この場合、該当する接続相手先のDoS攻撃防御の設定を［OFF］にしてご利用下さい。
　（☞「接続相手先ごとに、DoS攻撃防御機能のON/OFFを設定する」〈P.138〉）

本製品で防御するDoS攻撃について

FIN Scan

TCP FINフラグがオンになっているパケットを送信して、ポートをスキャンします。
本製品ではTCP通信を監視し、パケットのFINフラグが不正にオンになっているパケットを破棄します。

Null Scan

TCPフラグをすべてオフにしたパケットを送信して、ポートをスキャンします。
本製品では、パケットのフラグをチェックし、すべてオフになっているパケットを破棄します。

Xmas Scan（Nmap Xmas Scan）

URG、PSH、FINフラグがすべてオンのパケットを送信し、ポートをスキャンします。
本製品では、上記のフラグをチェックし、すべてオンになっているパケットを破棄します。

Smurf攻撃

送信元アドレスを偽造したICMP echo requestパケットをブロードキャストすることにより、大量のICMP echo replyパケットを、相手先に返送させるという仕組みの攻撃です。
本製品では、ブロードキャストアドレス宛てのICMP echo requestパケットを破棄します。また、IPアドレスが、本製品のサブネットと同じかどうかをチェックして、同じである場合、偽造アドレスとみなし、そのパケットを破棄します。

Ping of Death攻撃

Pingコマンドを使って不正なサイズのIPパケットを送信することにより、相手先の処理を不能にする攻撃です。
本製品では、IPパケットのサイズをチェックして、不正なサイズのパケットを破棄します。

Teardrop攻撃

断片化されたIPパケット（IPフラグメンテーションパケット）を再構築する際の、TCP/IP の実装上の問題に対する攻撃です。IPフラグメンテーションパケットには、再構築時に使用されるオフセット情報が含まれますが、そのオフセット情報を偽造することで、相手先の処理を不能にします。
本製品では、オフセット情報をチェックし、同じオフセット番号のパケットを破棄することにより、そのIPアドレスからのセッションを遮断します。

IP Spoofing攻撃

送信元のIPアドレスを、相手先のIPアドレスに偽装することによる攻撃です。
本製品では、送信元のIPアドレスをチェックし、プライベートIPアドレスの場合、そのパケットを破棄します。

Land攻撃

送信元と送信先に同じIPアドレスを持つパケットを相手先に送信することにより、相手先のパフォーマンスを低下させたり、処理不能にしたりする攻撃です。
本製品では、送信元と送信先のアドレスが同一かどうかをチェックし、同一のパケットを破棄します。

IP with Zero Length攻撃

IPパケットの最初のフラグメンテーションに、長さゼロのパケットを「おとり」として送信し、その後悪影響を及ぼすパケットを送り込むことで、相手先を攻撃します。
本製品では、パケットの最初のフラグメンテーションの長さ情報チェックし、ゼロの場合、そのパケットを破棄します。

Fraggle（UDP loop）

送信元のIPアドレスを偽造し、UDPのecho requestパケットをブロードキャストすることにより、相手先のパフォーマンスを低下させたり、処理不能にしたりする攻撃です。Echo、Chargen、Daytime、Qotdの各ポートが利用されます。
本製品では、ブロードキャストアドレス宛てのUDP echo requestパケットを破棄します。また、送信元のIPアドレスが、本製品のサブネットと同じかどうかをチェックして、同じである場合、偽造アドレスとみなし、そのパケットを破棄します。
また、送信元と送信先のポート番号が、7（Echo）、19（Chargen）、13（Daytime）、17（Qotd）の組み合わせである場合、そのパケットを破棄します。

拡張機能編

Snork攻撃

送信先ポート番号が135、送信元ポート番号が7（Echo）、19（Chargen）、13（Daytime）、135のいずれかのUDPパケットを送信し、不正に処理を繰り返させる攻撃です。
本製品では、このようなパケットをすべて破棄します。

リロード攻撃

Webページを連続してリロードすることにより、相手先に負荷を与える攻撃です。
本製品では、確立されたセッション数をカウントし、上限値を超えると、そのIPアドレスからのセッションを遮断します。

Fragment Flood

断片化されたパケットを大量に送信することにより、相手先を処理不能にする攻撃です。
本製品では、送信元のIPアドレスごとに、断片化されたパケット数をカウントし、設定した上限値を超えると、そのIPアドレスからのセッションを遮断します。

Connection Flood

長時間オープン状態にし続けることにより、相手先のソケットを占拠する攻撃です。
本製品では、一定時間アイドル状態のまま確立されたセッション数をカウントし、上限値を超えると、そのIPアドレスからのセッションを遮断します。

Ping Flooding

大量のICMP echo requestパケットを送信し、相手先のパフォーマンスを低下させる攻撃です。
本製品では、ICMP echo requestパケット数をカウントし、設定した上限値を超えるとそのIPアドレスからのICMP echo requestパケットを破棄します。

SYN Flood

SYNフラグがオンになっているTCPパケットを連続的に送信することにより、ハーフオープン状態のセッションを増加させ、相手先を処理不能にする攻撃です。
本製品では、SYNフラグがオンになっているTCPパケットの数、およびハーフオープン状態のセッション数をカウントし、設定した上限値を超えるとそのパケットを破棄します。

UDP Flood

大量のUDPパケットを送信し、相手のパフォーマンスを低下させる攻撃です。
本製品ではUDPパケット数をカウントし、設定した上限値を超えるとそのIPアドレスからのUDPパケットを破棄します。

DoS攻撃防御機能をONにする

本製品でDoS攻撃防御機能を使用する場合は、次の手順で設定します。

設定ページ

1 ［詳細設定］→［セキュリティ設定］→［ルータ］をクリックして、セキュリティ設定（ルータ）画面を開きます。

2 ［DoS攻撃防御設定］の［DoS攻撃防御］で［する］を選択すると、以下のDoS攻撃が防御されます。

・FIN Scan
・Xmas Scan（Nmap Xmas Scan）
・Ping of Death攻撃
・IP Spoofing攻撃
・IP with Zero Length攻撃
・Snork攻撃
・Fragment Flood
・Ping Flooding
・UDP Flood
・Null Scan
・Smurf攻撃
・Teardrop攻撃
・Land攻撃
・Fraggle（UDP loop）
・リロード攻撃
・Connection Flood
・SYN Flood

また、［ログ出力］で［する］をチェックすると、DoS攻撃防御機能のログを出力することができます。

3 ［オプション］欄にコマンドを入力して、以下の防御機能を設定することができます。

※{ }で囲まれている部分はパラメータです。パラメータの区切りには、半角スペースを入力して下さい。

※［オプション］欄で以下の防御機能を利用する設定を行っても、［DoS攻撃防御設定］の［DoS攻撃防御］で［する］を選択しなければ有効になりません。

ICMPフラッディング保護機能		
コマンド		ip dos icmpflood mode {on｜off}
	機能	ICMPフラッディング保護機能を利用するかどうかの設定
	説明	ICMPフラッディング保護機能を利用するかどうか設定します。 この機能により防御できるのは、Ping Floodです。
	パラメータ	**on　利用する** off　利用しない
コマンド		ip dos icmpflood echo {number}
	機能	ICMP echo requestパケット数の設定
	説明	ICMP echo requestパケット数がこの値を超えると、フラッディングブロックタイム〈P.137〉が経過するまで、そのIPアドレスからのICMP echo requestパケットが破棄されます。
	パラメータ	number ICMP echo requestパケット数（10～50） （購入時設定:**30**）

TCPインコンプリートセッション保護機能		
コマンド		ip dos incomplete mode {on｜off}
	機能	TCPインコンプリートセッション保護機能を利用するかどうかの設定
	説明	この機能によりSYN Floodを防御することができます。
	パラメータ	**on　利用する** off　利用しない
コマンド		ip dos incomplete session high {session}
	機能	上限インコンプリートセッション数の設定
	説明	この値を超えるハーフオープン状態のセッションが検出されると、ポート番号に関わらず、すべてのTCPセッションが遮断されます。
	パラメータ	sessionインコンプリートセッション数の上限（1～300） （購入時設定:**300**）
コマンド		ip dos incomplete session low {session}
	機能	下限インコンプリートセッション数の設定
	説明	TCPインコンプリートセッション保護機能によりTCPセッションが遮断された後、ここで設定した値までハーフオープン状態のセッション数が減少したら、セッションを再開します。
	パラメータ	sessionインコンプリートセッション数の下限（1～250） （購入時設定:**250**）

TCP/UDP非アクティブセッション保護機能		
本製品では、常にTCP/UDP非アクティブセッション保護機能がONになっています。 この機能では、非アクティブ状態のセッション数をカウントし、非アクティブセッション数が設定された上限値を超えると、そのセッションを遮断します。 これにより、以下の攻撃に対応できます。 ・Connection Flood　・リロード攻撃 ・UDP Flood		
コマンド		ip dos inactive session high {session}
	機能	上限非アクティブセッション数の設定
	説明	非アクティブセッション数がこの値を超えると、そのセッションは遮断されます。
	パラメータ	session非アクティブセッション数の上限（1～250） （購入時設定:**250**）
コマンド		ip dos inactive session low {session}
	機能	下限非アクティブセッション数の設定
	説明	非アクティブセッション保護機能によりセッションが遮断された後、ここで設定した値まで非アクティブセッション数が減少したら、セッションを再開します。
	パラメータ	session非アクティブセッション数の下限（1～200） （購入時設定:**200**）

同一ホストインコンプリート、非アクティブセッション保護機能		
コマンド		ip dos host incomplete mode {on｜off}
	機能	同一ホストインコンプリート、非アクティブセッション保護機能を利用するかどうかの設定
	説明	この機能を利用すると、同一IPアドレスからのハーフオープン状態で非アクティブなセッションがチェックされます。 これにより、同一ホストからの下記の攻撃に対応できます。 ・SYN Flood　・リロード攻撃 ・Connection Flood　・UDP Flood
	パラメータ	**on　利用する** off　利用しない
コマンド		ip dos host incomplete time {time}
	機能	インコンプリート、非アクティブセッション検出時間の設定
	説明	ここで設定した時間ごとに、インコンプリート、非アクティブセッションがチェックされます。
	パラメータ	timeインコンプリート、非アクティブセッション検出時間 （50～5000ミリ秒）（購入時設定:**300**ミリ秒）
コマンド		ip dos host incomplete session {session}
	機能	同一インコンプリート、非アクティブセッション数の設定
	説明	この値を超える、ハーフオープン状態、または非アクティブTCPセッションとUDPセッションが検出されると、そのIPアドレスからのセッションは遮断されます。 その後、フラッディングブロックタイム〈次ページ〉で指定した時間を経過した時点で、そのホストとのセッションが再開されます。
	パラメータ	sessionインコンプリートセッション数（1～50） （購入時設定:**10**）

同一ホストフラグメンテーション保護機能		
コマンド		ip dos host fragment mode {on｜off}
	機能	同一ホストフラグメンテーション保護機能を利用するかどうかの設定
	説明	この機能を利用すると、同一IPアドレスからの断片化されたパケットがチェックされます。これにより、同一ホストからのFragment Floodに対応できます。
	パラメータ	**on　利用する** off　利用しない
コマンド		ip dos host fragment time {time}
	機能	フラグメンテーション検出時間の設定
	説明	ここで設定した時間ごとに、同一IPアドレスからの断片化されたパケットがチェックされます。
	パラメータ	timeフラグメンテーション検出時間（10～60000ミリ秒） （購入時設定：**10000**ミリ秒）
コマンド		ip dos host fragment packet {packet}
	機能	同一ホストフラグメンテーションパケット数の設定
	説明	この値を超える、断片化されたパケットが検出されると、そのホストからのセッションは遮断されます。 その後、フラッディングブロックタイム〈下記参照〉で指定した時間を経過した時点で、そのホストとのセッションが再開されます。
	パラメータ	packetフラグメンテーションパケット数（1～150） （購入時設定：**30**）

フラッディングブロックタイム		
コマンド		ip dos blocktime {time}
	機能	フラッディングブロックタイムの設定
	説明	フラッディング攻撃が防御され、セッションが遮断されたとき、何秒間遮断するかを設定します。
	パラメータ	time ブロックタイム（60～30000秒） （購入時設定：**300**秒）

（設定例1）　ICMPフラッディング保護機能を利用し、ICMP echo requestパケット数を40、フラッディングブロックタイムを400秒にする場合

```
ip dos icmpflood mode on
ip dos icmpflood echo 40
ip dos blocktime 400
```

拡張機能編

（設定例2）　TCPインコンプリートセッション保護機能を利用し、下限セッション数を20、上限セッション数を80にする場合

ip dos incomplete mode on
ip dos incomplete session low 20
ip dos incomplete session high 80

（設定例3）　同一ホストインコンプリート、非アクティブセッション保護機能を利用し、セッション数を20、検出時間を600にする場合

ip dos host incomplete mode on
ip dos host incomplete session 20
ip dos host incomplete time 600

（設定例4）　同一ホストフラグメンテーション保護機能を利用し、パケット数を20、検出時間を5000にする場合

ip dos host fragmentation mode on
ip dos host fragmentation packet 20
ip dos host fragmentation time 5000

4. ［設定］ボタンをクリックします。

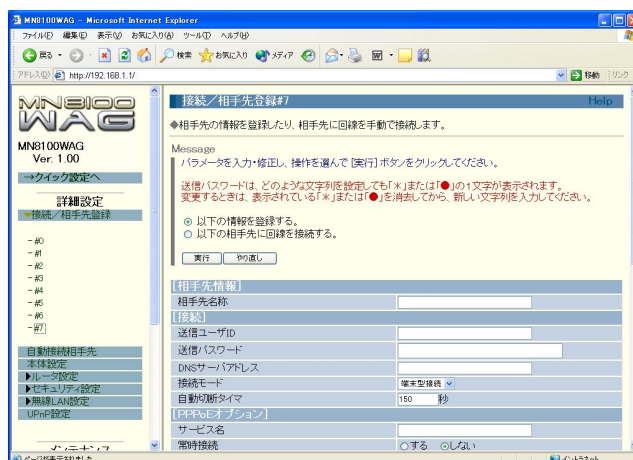
すべての接続先に対して、設定した内容が有効になります。
接続した相手先ごとに、DoS攻撃防御機能のON/OFFを設定したい場合は、次の手順に従って行って下さい。

接続相手先ごとに、DoS攻撃防御機能のON/OFFを設定する

購入時の設定では、［セキュリティ設定］画面で行ったDoS攻撃防御機能の設定は、すべての接続先に対して有効になります。
接続相手先によって、DoS攻撃防御機能を無効にしたい場合は、以下の手順で設定を変更します。

設定ページ

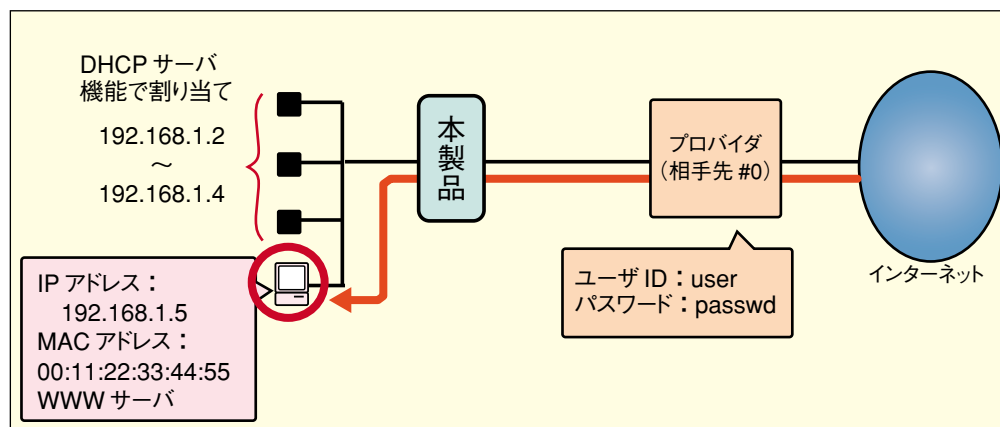
1. ［詳細設定］→［接続／相手先登録］で、設定したい接続先番号のページを開きます。

拡張機能編

2. 導入時の設定では、［DoS攻撃防御設定］の［DoS攻撃防御］/［ログ出力］で、［する］が選択されています。［しない］を選択すると、その接続相手先に対して、DoS攻撃防御機能/ログ出力機能がそれぞれ無効になります。

3. ［以下（以上）の情報を登録する。］を選択して、［実行］ボタンをクリックします。

   その相手先に対する設定が有効になります。

13 WWWサーバを公開する（端末型）

プロバイダにPPPoE端末型で接続したときに、こちら側のWWWサーバを公開する例を紹介します。

通常、プロバイダにPPPoE端末型で接続したときは、相手先からはこちらのサーバを利用することはできません。
本製品では、相手先に対して、WWWサーバの利用に必要なサービス（WWW、ftpなど）を使用できるように設定できます。相手先に各種サービスの利用を許可するには、IPアドレス変換（NAT）テーブルおよびIPフィルタを使います。IPアドレス変換（NAT）テーブルは32個、IPフィルタは64個まで設定できます。

◆インターネットにサーバを公開すると、外部からの攻撃などの被害に遭う可能性があります。セキュリティ対策を十分に行って下さい。

◆本製品にはステートフル・パケット・インスペクション（SPI）機能〈P.82〉が購入時の状態でONになっています。この機能をOFFにすると、IPフィルタを使用しないで各種サービスの利用を許可することができますが、セキュリティのレベルが下がるので注意して下さい。

設定ページ

■［詳細設定］→［接続／相手先登録］→［#0］

相手先名称	名称（何でも構いません）を設定
送信ユーザ ID	user
送信パスワード	passwd
接続モード	［端末型接続］を選択

■［詳細設定］→［ルータ設定］→［LAN］

オプション	ip filter 1 pass in * 192.168.1.5 tcp * www remote 0 ip nat 1 192.168.1.5/tcp/www ipcp remote 0 ip nat 2 */*/* ipcp remote 0 ip host 192.168.1.5 host.mn8100wag.co.jp 0a:1b:2c:00:11:22 （host.mn8100wag.co.jp：任意のホスト名を割り当てます。） （0a:1b:2c:00:11:22：パソコンのMACアドレスです。）

相手先は、本製品がIPCPで取得したIPアドレスを使って、こちら（本製品）側のWWWサーバにアクセスできます。なお、IPCPで取得したIPアドレスは、［メンテナンス］の［WAN接続状況］→［PPPoE］画面にある［割り当てIPアドレス］で確認できます。

このほか、セキュリティのためインターネット側からの不正パケット破棄したり、意図しない接続を禁止するIPフィルタの設定をすることをお勧めします。フィルタの設定については、「IPフィルタの設定」〈P.150〉をお読み下さい。

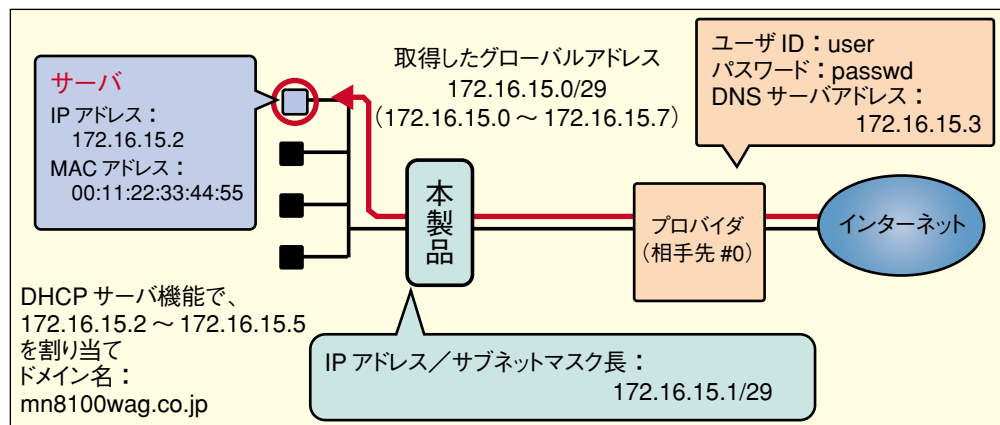
◆ PPPoE端末型接続時のIPアドレス変換（NAT）テーブルの登録

IPアドレス変換（NAT）を登録しなくても、本製品からPPPoE端末型でインターネットに接続すると、LAN上のすべてのパソコンから相手先にアクセスすることができます。これは、AutoNAT機能によって、すべてのプライベートIPアドレスが自動的に取得するグローバルIPアドレスに変換されるためです。IPアドレス変換（NAT）テーブルは必要に応じて登録して下さい。

◆ PPPoE端末型接続時や本製品に登録したNATテーブルを使った通信時のRIPについて

PPPoE端末型接続時や、WANポートに固定IPアドレスを設定したとき、DHCPサーバからIPアドレスを取得したときは、本製品に登録したNATテーブルを使った通信時に相手先にRIPを送信しません。

14 サーバを立ち上げて外部に公開する（NAT未使用）

ここでは、グローバルIPアドレスを複数取得してLANを運用し、WWW、FTP、DNS、メールサーバを公開する例をご紹介します。

※上記の場合、172.16.15.0、172.16.15.7は端末には割り当てられません。

インターネットにサーバを公開すると、外部からの攻撃などの被害に遭う可能性があります。セキュリティ対策を十分に行って下さい。

設定ページ

■［詳細設定］→［接続／相手先登録］→［#0］

相手先名称	名称（何でも構いません）を設定
送信ユーザ ID	user
送信パスワード	passwd
DNS サーバアドレス	172.16.15.3
接続モード	［LAN 型接続］を選択

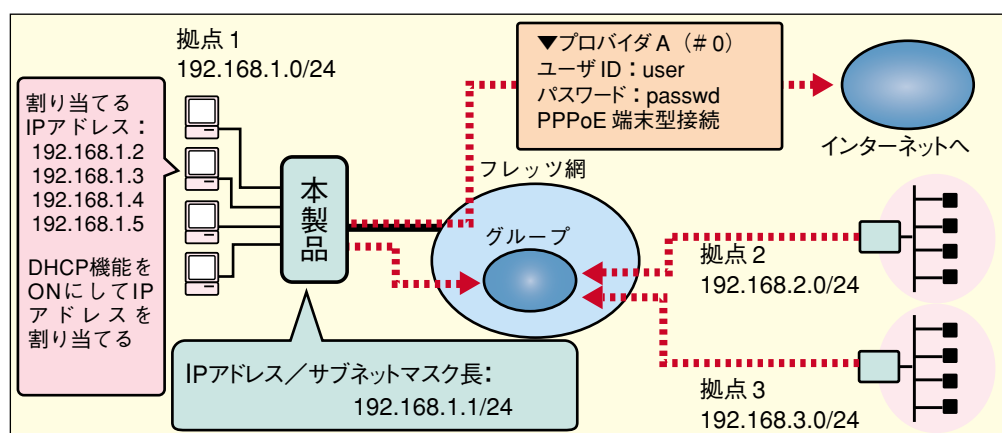
■［詳細設定］→［ルータ設定］→［LAN］

本体のIPアドレス/サブネットマスク長	172.16.15.1/29
DHCP サーバ機能	ON
開始 IP アドレス / 個数	172.16.15.2/4
ドメイン名	mn8100wag.co.jp
オプション	次のコマンドを設定 ip filter 20 pass in * 172.16.15.2 tcp * pop3 remote 0 ip filter 21 pass in * 172.16.15.2 tcp * www remote 0 ip filter 22 pass in * 172.16.15.2 tcp * 443 remote 0 ip filter 23 pass in * 172.16.15.2 tcp * smtp remote 0 ip filter 24 pass in * 172.16.15.2 tcp * domain remote 0 ip filter 25 pass in * 172.16.15.2 udp * domain remote 0 ip filter 26 pass in * 172.16.15.2 tcp * 113 remote 0 ip filter 27 pass in * 172.16.15.2 tcp * ftp remote 0 ip filter 28 pass in * 172.16.15.2 tcp * ftpdata remote 0 ip filter 29 pass in * 172.16.15.2 tcp * 1024-65535 remote 0 ip filter 30 pass in * 172.16.15.2 udp * 1024-65535 remote 0 ip filter 31 reject in * 172.16.15.2 udp * * remote 0 ip host 172.16.15.2 host.mn8100wag.co.jp 00:11:22:33:44:55 （host.mn8100wag.co.jp：任意のホスト名を割り当てます。）（00:11:22:33:44:55：パソコンのMACアドレスです。）

※IP filter21、22はWWWサーバへのアクセスを通すためのフィルタです。
※IP filter20、23、26はメールサーバへのアクセスを通すためのフィルタです。
※IP filter24、25はDNSへのアクセスを通すためのフィルタです。
※IP filter27、28はftpdataとftpパケットを通すためのフィルタです。
※IP filter29、30は外部からの送信ポートが1024番以降（WellKnownポート以外）を通すためのフィルタです。
※IP filter31は上記以外のアクセスを破棄するためのフィルタです。

このほか、セキュリティのためインターネット側からの不正パケット破棄したり、意図しない接続を禁止するIPフィルタの設定をすることをお勧めします。フィルタの設定については、「IPフィルタの設定」〈P.150〉をお読み下さい。

15 フレッツ・グループアクセスを利用する

フレッツ・グループアクセス（NTT東日本）、またはフレッツ・グループ（NTT西日本）は、フレッツ・ADSL、Bフレッツ利用者同士によるグループ内通信を可能とするサービスです。フレッツ・グループアクセス（NTT東日本）のサービスメニューには、「フレッツ・グループアクセス・プロ」と「フレッツ・グループアクセス・ライト」の2つがあります。同様にフレッツ・グループ（NTT西日本）のサービスメニューには、「ベーシックメニュー」と「ビジネスメニュー」の2つがあります（2004年6月現在）。
ルータを利用してそれぞれのサービスを利用する場合は、LAN型払い出しのできるフレッツ・グループアクセス・プロ（NTT東日本の場合）、またはビジネスメニュー（NTT西日本の場合）を利用するとよいでしょう。
ここでは、フレッツ・グループアクセス・プロを契約して、メインセッションはプロバイダへ接続、サブセッションでフレッツ・グループアクセスへPPPoEで接続する例を解説します。

設定ページ

■プロバイダに接続するための設定

● ［クイック設定］→［PPPoE（端末型）］

ログインユーザ ID	設定ページを開くためのユーザ ID を入力します。
ログインパスワード	設定ページを開くためのパスワードを入力します。
ログインパスワード（再入力）	上記で設定したパスワードをもう一度入力します。
PPPoE（端末型）設定：メイン 以下の内容で設定を行う	チェックする
相手先名称	名称（何でも構いません）を設定
送信ユーザ ID	user
送信パスワード	passwd

ログインユーザIDとログインパスワードは、インターネット側から本製品の設定ページへ不正にアクセスできないようにするために設定します。
［PPPoE（端末型）設定：メイン］で、契約しているプロバイダの設定を行います。

拡張機能編

■フレッツ・グループアクセスの設定

● ［詳細設定］ → ［接続／相手先登録］ → ［＃7］

相手先名称	名称（何でも構いません）を設定
送信ユーザ ID	フレッツ・グループアクセス・プロで割り当てられたユーザID を入力
送信パスワード	フレッツ・グループアクセス・プロで割り当てられたパスワードを入力
接続モード	［LAN 型接続］を選択 ※端末型IPアドレス払い出しの契約を行った場合は［端末型接続］を選択して下さい。

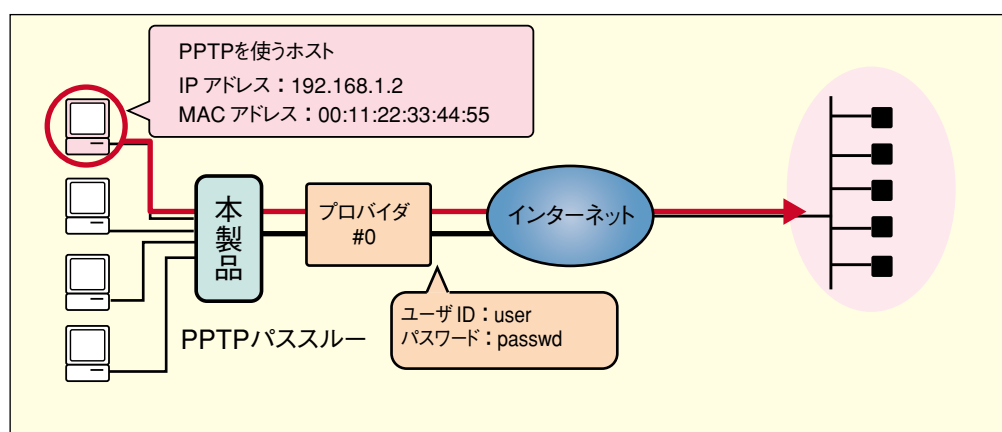
● ［詳細設定］ → ［ルータ設定］ → ［LAN］

本体のIPアドレス/サブネットマスク長	192.168.1.1/24 ※フレッツ・グループアクセス・プロで割り当てられたIPアドレスを設定します。
DHCPサーバ機能	ONを選択
開始IPアドレス/個数	192.168.1.2/4 ※フレッツ・グループアクセス・プロで割り当てられたIPアドレスを設定します。 ※割り当てるIPアドレスのうち、最初のIPアドレスと、割り当てるIPアドレスの個数を入力します。
オプション	ip filter 1 pass out 192.168.1.1-192.168.1.5 * * remote 7 ip filter 2 pass in 192.168.2.0/24 * * remote 7 ip filter 3 pass in 192.168.3.0/24 * * remote 7 ip filter 4 reject out * * * remote 7 ip filter 5 reject in * * * remote 7 ip route 192.168.2.0/24/2 remote 7 static ip route 192.168.3.0/24/2 remote 7 static

メインセッションでPPPoE（LAN型）を設定した場合、サブセッションでフレッツ・グループ・アクセスを利用することはできません。

16 VPNを構築する

VPNパススルー

本製品は、VPNのプロトコルをIPアドレス（変換）テーブルを作成しなくても自動的に設定して通過させることができる、「VPNパススルー」機能を搭載しています。本製品は、IPsec、PPTP、L2TPの3種類のプロトコルに対応しています。
ここでは、PPPoE端末型でインターネットに接続し、LAN内の特定のパソコンでPPTPで通信を行う場合の設定を解説します。

設定ページ

■プロバイダに接続するための設定

● ［詳細設定］ → ［接続／相手先登録］ → ［#0］

相手先名称	名称（何でも構いません）を設定
送信ユーザ ID	user
送信パスワード	passwd
接続モード	［端末型接続］を選択

■VPNパススルーの設定

LAN上にVPNのサーバを設置する場合は、［LAN側のホストアドレス］を必ず設定して下さい。なお、LAN側のホストアドレスを設定すると、そのIPアドレスのパソコン以外は、VPN（IPsec、PPTP、L2TP）による通信ができません。

●［詳細設定］→［セキュリティ設定］→［ルータ］

PPTP パススルー	［透過する］を選択
LAN 側 PPTP ホストアドレス	192.168.1.2

●［詳細設定］→［ルータ設定］→［LAN］

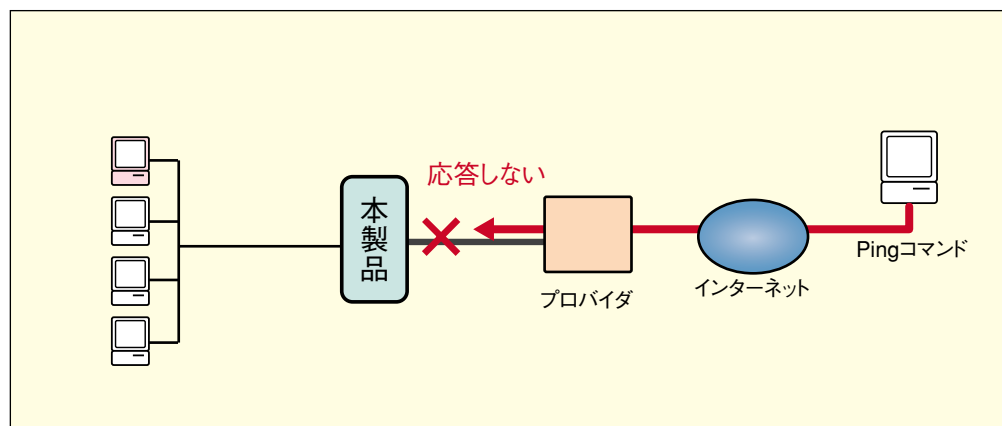
オプション	ip host 192.168.1.2 user1.mn8100wag.co.jp 00:11:22:33:44:55 （user1.mn8100wag.co.jp：任意のホスト名を割り当てます。） （00:11:22:33:44:55：パソコンのMACアドレスです。）

LAN側のホストアドレスを指定しなかった場合は、LAN内の複数のパソコンでVPN（IPsec、PPTP、L2TP）による通信が可能になります。各プロトコルの最大セッション数は1となります。ただし、同一相手先へ同時に接続することはできません。また、この場合、インターネット側から接続を開始することはできません。

17 ルータ機能のセキュリティ

本製品には、セキュリティ対策の機能として「ステルスモード」「SPI」「IPフィルタ」機能が用意されています。ただし、これらの機能を使用していても、絶対に被害に遭わないということはありません。十分にご注意下さい。

ステルスモードにする

ステルスモードにすると、インターネットからPINGコマンドに応答しなくなり、またインターネットへのICMPエラーやTCPのリセットを返さなくります（ポート113を除く）。これにより、外部に本製品の存在を隠すことができ、ポートスキャンなどの攻撃から守ることができます。応答せずに破棄したパケットのログを［メンテナンス］の［情報表示］→［ログ］に出力可能です。

設定ページ

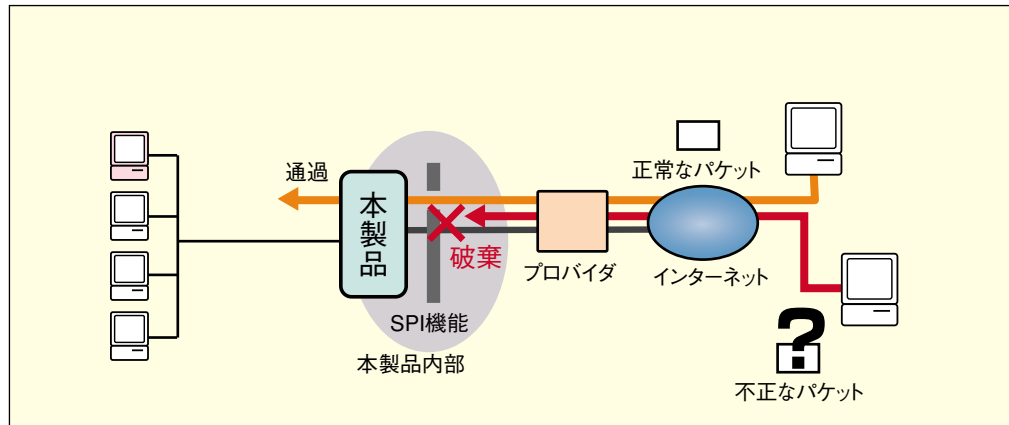
■［詳細設定］→［セキュリティ設定］→［ルータ］

ステルスモード	ON
ログ出力	する

■［詳細設定］→［セキュリティ設定］→［ログ通知］

ログ出力レベル	［NOTICE］をチェック

SPI機能を使う

「SPI（ステートフル・パケット・インスペクション）」とは、受信したパケットの内容や通信の状態を監視して、自動的にポートの開放・閉鎖を行う機能です。SPI機能を使うと、不正な手段で送信されたパケットを破棄することができます。

設定ページ

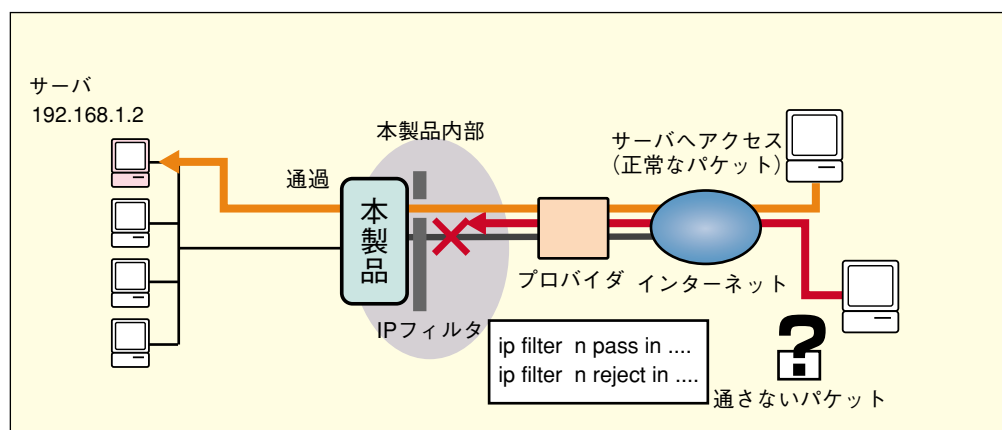
■［詳細設定］→［セキュリティ設定］→［ルータ］

SPI	ON
ログ出力	する

■［詳細設定］→［セキュリティ設定］→［ログ通知］

ログ出力レベル	［NOTICE］をチェック

IPフィルタの設定

IPフィルタは、送信元や送信先、ポート番号、通信の方向などの条件を設定して、本製品に送られてきたパケットを通過させるか拒否するかを判断する機能です。LAN側からインターネットへの意図しない接続を防ぐ設定もできます。

FTTH、ADSL、CATV、フレッツなど、常時インターネットできる環境では、外部からの不正アクセスや攻撃にさらされる危険性も高くなります。IPフィルタ機能を使って、LAN内に通す・通さないパケットを指定して、セキュリティ対策を十分に行う必要があります。

本製品には、購入時の設定でいくつかのフィルタが設定されているほか、クイック設定を行うと、自動的にフィルタが設定されます。詳しくは、「クイック設定で自動的に設定されるフィルタ」〈P.190〉をお読み下さい。

IPフィルタは、［詳細設定］→［ルータ設定］→［LAN］の［オプション］欄にコマンドを次の書式で入力することで設定できます。

ip filter {fnumber type dir srcaddr dstaddr protocol srcport dsport interface [rnumber] [log]}

パラメータ	値	説明
fnumber		フィルタ番号 1～64の間で設定します。 番号の小さい方の設定が優先されます。
type	 pass reject restrict	フィルタのタイプ 一致すればパケットを通す 一致すればパケットを破棄する 回線が接続されている場合だけパケットを通す
dir	 in out	方向 受信時にフィルタリングする 送信時にフィルタリングする
srcaddr		送信元アドレス[/ネットマスク¦-範囲指定] 「*」を入力するとすべてのIPアドレスが対象になります。 範囲を指定するときは、「-」で入力します。
dstaddr		送信先アドレス[/ネットマスク¦-範囲指定] 「*」を入力するとすべてのIPアドレスが対象になります。 範囲を指定するときは、「-」で入力します。
protocol	 ニーモニック	プロトコル番号、またはニーモニック 「*」を入力するとすべてが対象になります。 範囲を指定するときは、「-」で入力します。 esp、gre、icmp、ipencap、tcp、tcpest、tcpfin、udp、tcp_udp tcpestはSYN、tcpfinはFIN/RSTパケットを対象とします。
srcport	 ニーモニック	送信元ポート番号、またはニーモニック 「*」を入力するとすべてが対象になります。 範囲を指定するときは、「-」で入力します。 ftp、ftpdata、telnet、smtp、www、pop3、sunrpc nntp、ntp、login、pptp、domain、route、who ※プロトコルに「*」を指定した場合は記述しません。
dstport		送信先ポート番号、またはニーモニック 「*」を入力するとすべてが対象になります。 範囲を指定するときは、「-」で入力します。 ※プロトコルに「*」を指定した場合は記述しません。
interface	local remote wanether wanany	LAN側のフィルタ WAN側（接続相手-PPTP、PPPoE）のフィルタ WAN側（DHCPサーバからのアドレス取得、手動による固定IPアドレスの設定）のフィルタ すべてのWAN側のフィルタ
rnumber		相手先番号 0～7で指定します。 remoteの場合は、「*」ですべての相手先を指定できます。
log	 nolog	ログタイプ ログを出力しない

拡張機能編

設定ページ

■［詳細設定］→［ルータ設定］→［LAN］

●相手先#1から「192.168.1.2」のFTPサーバだけのアクセスを許可する

オプション	ip filter 1 pass in * 192.168.1.2/32 tcp * ftpdata-ftp remote1 ip filter 2 reject in * * * remote1

●WWWでのアクセスを許可する

オプション	ip filter 1 pass in * 192.168.1.2/32 tcp * www remote1

本製品のIPフィルタ機能は、番号の小さい順から参照して条件に一致したものから処理していきます。内容によっては設定順を間違えると、フィルタが無効になるので注意して下さい。たとえば、「インターネット側からのTCPアクセスをすべて禁止する」フィルタが上位に設定されている場合、その下に特定のTCPパケットを通す設定をしても有効にはなりません。

次のような例では、フィルタ58ですべてのTCPパケットが破棄されるので、フィルタ59を設定してもインターネット側からWWWサーバにアクセスすることはできません。

オプション	ip filter 58 reject in * * tcpest * * remote 1 （インターネット側からLAN内へのTCPアクセスを禁止） ip filter 59 pass in * 192.168.1.2/32 tcp * www remote 1 （「192.168.1.2」宛てのwwwパケットを通す）

次のようにフィルタの順序を逆にすると、フィルタ58で「192.168.1.2」宛てのwwwパケットを通し、フィルタ59でそれ以外のTCPパケットを破棄するようになります。

オプション	ip filter 58 pass in * 192.168.1.2/32 tcp * www remote 1 （「192.168.1.2」宛てのwwwパケットを通す） ip filter 59 reject in * * tcpest * * remote 1 （インターネット側からLAN内へのTCPアクセスを禁止）

フィルタの登録順位は、先に条件を限定しているフィルタ、最後に条件を広範囲にしているフィルタに設定します。
インターネット側から受け取ったパケットの処理は、基本は「reject in（破棄）」、必要なものだけ「pass in（受信）」と考えるとよいでしょう。

18 無線LANのセキュリティ

無線LANを安全に使うポイント

■無線LANのセキュリティ問題について

無線LANは、配線や特別な設定なしにすべてのパソコンや機器が相互に通信ができるように設計されています。反面、セキュリティの設定をしないと、無線LANの電波が届く範囲内であれば誰でも簡単に、通信内容を傍受、あるいはネットワークに侵入することが可能になるという問題があります。無線LANをお使いの場合は、有線のLAN以上にセキュリティ対策を十分に行うことをお勧めします。

■無線LANのセキュリティ機能の種類

上記の問題を防ぐため、本製品では下記のセキュリティ機能が準備されています。セキュリティを強固するには下記1)、2)の両方を組み合わせて設定する必要があります。

1）無線LAN接続関連のセキュリティ機能

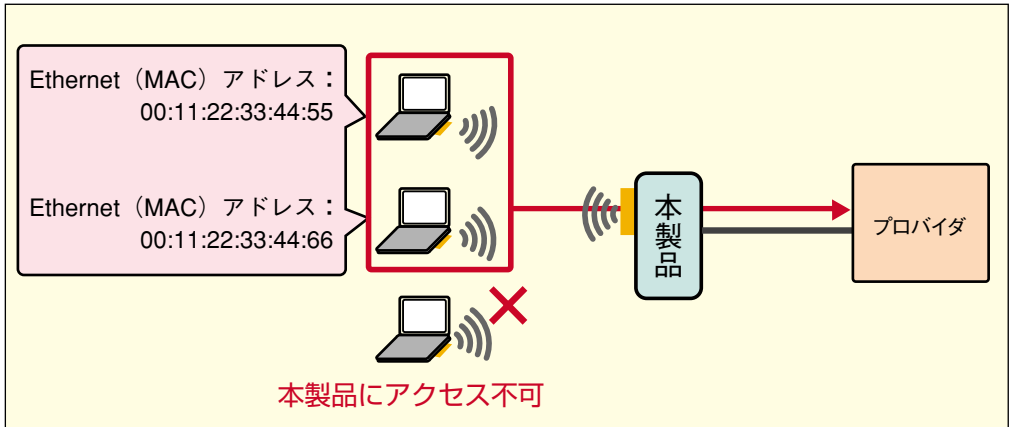
セキュリティ機能	概要
SSID（Service Set Identifier）	接続先の無線LANアクセスポイントを指定するIDで、同じSSIDを設定した無線LAN端末だけが接続可能になります。
無線LANステルス機能	SSIDが空白、またはANYに設定されているパソコンからの応答を禁止（ANYプローブ応答禁止）し、これらのパソコンとの接続を拒否（ANY接続拒否）します。この場合SSIDをほかのパソコンから検索できなくなります（SSIDの隠蔽）。
MACアドレスフィルタリング	個々の無線LAN端末が持つ端末固有の番号（MACアドレス）を本製品にあらかじめ登録することで、登録されている無線LAN端末だけを接続可能にします。

2）暗号化機能

セキュリティ機能	概要
WEP （Wired Equivalent Privacy）	共通の暗号化キー（WEPキー）で本製品と無線LAN端末間のデータを暗号化します。
WPA-PSK （Wi-Fi Protected Access）	本製品がWPA共有キーを用いてユーザ認証を行います。WEPより強力な、TKIP（Temporal Key Integrity Protocol）、AES（Advanced Encryption Standard）と言う暗号化機能が採用されております。

接続できる無線LAN端末を制限する

無線で本製品に接続できる無線LAN端末を限定するときは、相手の無線LAN端末のMACアドレスを登録します。MACアドレスを登録すると、それ以外の無線LAN端末とは通信できません。これにより、意図しない第三者が勝手に本製品を利用するのを防ぐことができます。

登録したMACアドレスを持つパソコン以外が、本製品に接続するのを禁止する機能です。外部からの侵入を防ぐことができますが、盗聴防止には効果はありません。また専用のツールでMACアドレスを盗聴される可能性があり、暗号化機能とあわせて使用することを推奨します。

設定ページ

■［詳細設定］→［無線LAN設定］→［MACアドレスフィルタリング］

接続許可	［リストの無線 LAN 端末を許可］にチェック
MAC アドレス	登録したい MAC アドレスを入力 ※ 32 件まで登録できます。

◆パソコンに取り付けた無線LANカードのMACアドレスを確認する

各パソコンでMACアドレスを確認できます。操作方法は「パソコンのMACアドレスを確認する」〈P.123〉を参照して下さい。

拡張機能編

WEPを設定し、暗号化通信を行う

WEPを設定することで、無線電波が第三者に傍受されても、暗号を解読しないとデータの中身を判読することができなくなり、また無線LANに侵入することもできません。WEP機能はパソコン等および本製品の両方にWEPキーを設定する必要があります。本製品では64bit、128bit、152bit長のWEPキーをサポートしています。各ビット長の内、設定できるWEPキー長は、それぞれ「40bit（5Byte）」「104bit（13Byte）」「128bit（16Byte）」となります。残りの24ビットはIV（Initialization Vector）と言われる自動的にパソコンや無線LAN端末により付加されるデータとなります。設定されるWEPキーの長さが長いほど、暗号は強力となります。WEP認証方式には、それぞれ「オープンシステム認証」と「共有キー認証」を選択することができます。お使いの無線LAN端末の規格を確認して下さい。

◆オープンシステム認証を選択した場合
無線LAN端末からは資格情報無しに認証依頼を行い、本製品は依頼された認証をそのまま受け入れます。そのため、基本的には認証は行われていません。

◆共有キー認証を選択した場合
本製品と無線LAN端末はWEPキーを用いた認証を行います。

万が一WEPキーが破られることを想定して、定期的にWEPキーを変更することを推奨します。

設定ページ

1. ［詳細設定］→［無線LAN設定］→［IEEE802.11a］または［IEEE802.11g/b］をクリックして、無線LAN設定画面を開きます。

拡張機能編

2.［セキュリティ］の項目で、次のように設定します。

認証・暗号化	［WEP］をクリック

3.［WEP］の項目でWEPキーに関する設定をします。

WEP 認証方式	［オープンシステム認証］または［共有キー認証］にチェック ※セキュリティ上、［共有キー認証］をチェックすることをお勧めいたします。
WEP キーの長さ	［64bit］［128bit］［152bit］のいずれかを選択
キーインデックス	［1］～［4］のいずれかを選択

◆WEP認証方式は通常、無線LAN端末側が自動的に判別します。

◆Windows XP SP1環境でWireless Zero Configをご使用の場合、［ネットワーク認証(共有モード)］のチェックを外すと、オープンシステム認証となります。チェックを入れると共有キー認証となります。本製品の設定と同じ設定内容にして下さい。

4 ［WEPキー1］、［WEPキー2］、［WEPキー3］、［WEPキー4］にWEPキーを設定します。
［WEPキーの長さ］の設定により入力できる文字数が異なります。

	16 進数 (0～9、a～f までの 16 進数)	ASCII 入力 (半角英数字)
64bit	10 文字 例：12:34:56:78:90	5 文字 例：A1b2C
128bit	26 文字 例：12:34:56:78:90:ab:cd:ef:12:34:56:78:90	13 文字 例：A1b2C3d4E5f6G
152bit	32 文字 例：12:34:56:78:90:ab:cd:ef:12:34:56:78:90:ab:cd:ef	16 文字 例：A1b2C3d4E5f6G7h8

◆認証・暗号化に［WEP］を選択したときは、必ずWEPキーを設定して下さい。WEPキーを設定していないと、通信ができなくなります。また、設定したWEPキーは忘れないようにして下さい。

◆本製品とパソコン側とで、同じWEPキーを設定して下さい。WEPキーが一致していないと通信ができなくなります。

◆「MN SS-LAN CARD/USB 11HQ」または「MN SS-LAN CARD 11 HQ-R」を使った無線LAN端末を利用する場合は、WEPキーを16進数で入力して下さい。

WPA-PSKを設定し、無線LANのセキュリティを強化する

WPAは従来の無線LANに比較して、以下の点が強化されています。

1.TKIP（Temporal Key Integrity Protocol）による強力な暗号化をサポートします。TKIPでは新しいキー生成アルゴリズムを用い、設定された仮共有キーであるWPA-PSKにより生成されたキーとIVおよびMACアドレスからキーを生成します。IVのビット長も48ビットに拡張され、キーは定期的に更新されます。キーが定期的に更新されることにより、無線LANの通信が盗聴され、キーが解読されたとしても、すぐにキーが更新されるので、WEPと比較して高いセキュリティを実現しています。
2.暗号アルゴリズムとしてAES（Advanced Encryption Standard）というアメリカ国務省標準技術局（NIST）が定めた新しい暗号アルゴリズムをオプションとして採用しています。

本製品ではWPA共有キーを利用する「WPA-PSK」が利用できます。ここではAESの設定例について解説します。

利用する無線LAN端末がWPA-PSKに対応している必要があります。
お使いの無線LANカードによっては、WPA-PSKを使用できるパソコンのOSが限定されている場合があります。詳しくは無線LANカードに付属の取扱説明書をお読み下さい。

設定ページ

1 ［詳細設定］→［無線LAN設定］→［IEEE802.11a］または［IEEE802.11g/b］をクリックして［無線LAN設定］画面を開きます。

2 ［セキュリティ］の項目で次のように設定します。

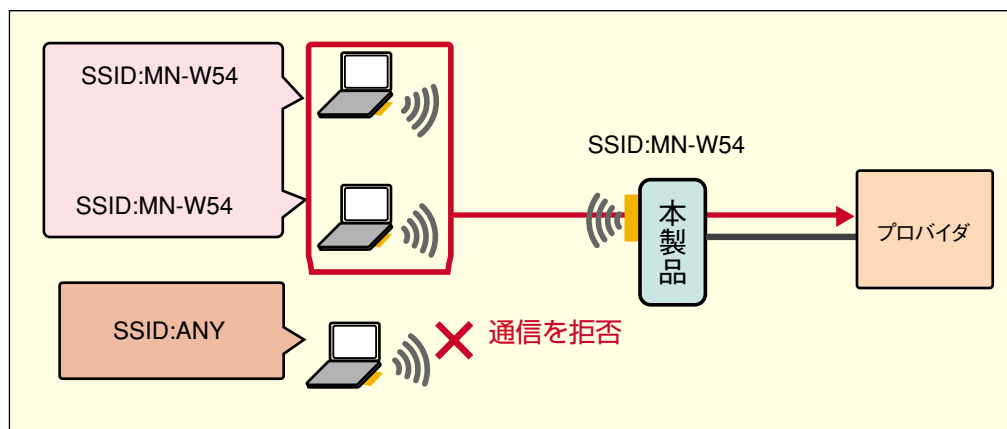
認証・暗号化	［WPA-PSK］をクリック

3 ［WPA-PSK］の項目で次のように設定します。

WPA 共有キー	1q2w3e4r5t6y7u8i ※ WPA 共有キーは半角英数で 8 ～ 63 文字の範囲内です。
暗号方式	［AES］を選択
キー更新間隔	3600 ※ 30 ～ 99999 の間で設定できます。 ※数値を小さくすると、鍵の更新が頻繁に行われるため、セキュリティは強固になりますが、スループットが低下します。 ※数値を大きくすると、鍵の更新間隔が空くため、セキュリティは弱くなりますが、スループットは向上します。

パソコン側の無線LANカードの設定方法については、対応無線LANカードの取扱説明書を参照して下さい。

SSIDが空白、または「ANY」に設定された パソコンとの通信を拒否する

SSIDとは、無線LANで通信相手を特定するための識別記号のことです。本製品と本製品に接続するパソコンで同じSSIDを設定することで、無線LANで通信できるようになります。
無線LANの仕様では、パソコン側で「ANY」や空欄にしておくと、どのようなSSIDでも接続できます。本製品の「無線LANステルス機能」を有効にすると、「ANY」や空白のSSIDでは本製品にアクセスできなくなります。また、Windows XPのワイヤレスネットワーク（Windows Zero Config）などから、設定しているSSIDを検索できなくなります。

設定ページ

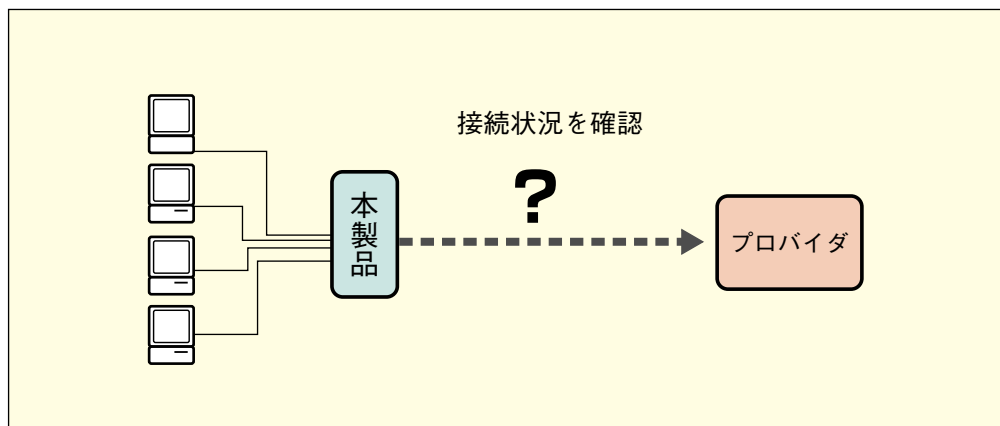
■［詳細設定］→［無線LAN設定］→［IEEE802.11a］または［IEEE802.11g/b］

SSID	MN-W54
無線 LAN ステルス機能	［有効］

無線LANステルス機能を無効にしている場合は、設定しているSSIDは第三者が簡単に見ることができるので、SSIDにセキュリティとしての機能は期待できません。逆にSSIDに自分の名前や組織名など利用者を特定できる名前を設定すると、第三者に不要な興味を抱かせる可能性があります。出来るだけ意味を持たない名前を設定するようにして下さい。

保守編

1 接続状況を確認する

設定ページから、チャネルの使用状況や、接続中の相手先を確認できます。例えば、すでにLANポートにつないだパソコンからインターネットにアクセスしているときは、その回線を使ってほかのパソコンもインターネットにアクセスすることができます。

PPPoEでの接続の場合

設定ページ

1. ［メンテナンス］の［WAN接続状況］→［PPPoE］をクリックします。
   ［WAN接続状況（PPPoE）］画面が表示されます。

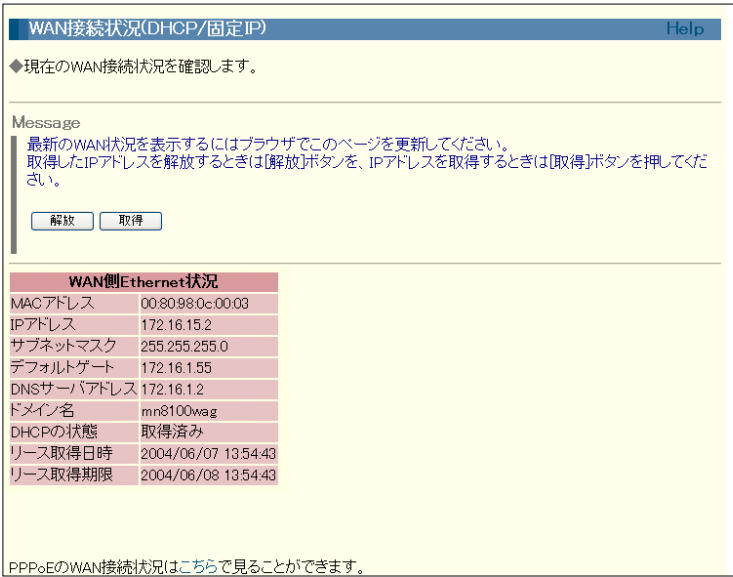
チャネル	PPPoE1
接続状況	接続中
接続時刻	2004/06/14 21:18:17
接続モード	端末型
リンクプロトコル	LCP IPCP
相手先ルータアドレス	218.227.247.199
相手先DNSサーバアドレス	202.225.94.247
割り当てIPアドレス	219.107.199.246
無通信時間/自動切断時間(秒)	36/なし
相手先登録番号	0
相手先名称	プロバイダ(メイン)

現在の接続状況が接続ごとに表示されます。

接続状況	回線が接続されているときは「接続中」、接続していないときは「空き」と表示されます。
接続時刻	接続を開始した時刻が表示されます。
接続モード	相手先と接続しているモードに応じて「端末型」または「LAN型」と表示されます。
リンクプロトコル	接続に使用されているプロトコルが表示されます。
相手先ルータアドレス	相手先（プロバイダ）のルータのIPアドレスが表示されます。
相手先DNSサーバアドレス	相手先（プロバイダ）のDNSサーバのIPアドレスが表示されます。
割り当てIPアドレス	端末型接続時に割り当てられる、グローバル IP アドレスが表示されます。 ※接続のたびに違うIPアドレスが割り当てられることがあるので、その都度確認して下さい。
無通信時間／自動切断時間（秒）	通信されていない時間と、設定されている自動切断までの時間が秒単位で表示されます。
相手先登録番号	［詳細設定］の［接続／相手先登録］に登録されている番号が表示されます。
相手先名称	［詳細設定］の［接続／相手先登録］に登録した番号内の［相手先名称］が表示されます。

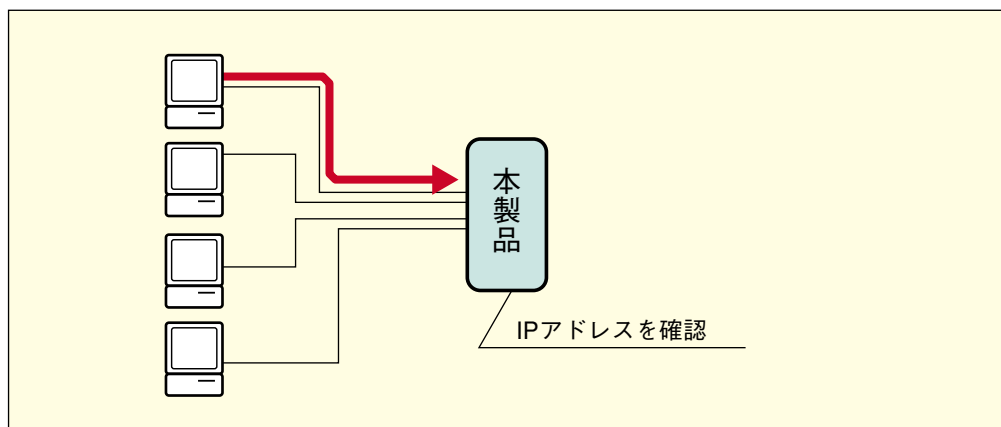
DHCP接続／固定IPアドレスでの接続の場合

設定ページ

1. ［メンテナンス］の［WAN接続状況］→［DHCP/固定IP］の順にクリックします。
   ［WAN接続状況（DHCP/固定IP）］画面が表示されます。

現在の接続状況が表示されます。

MAC アドレス	WANポートのMACアドレスが表示されます。
IPアドレス	接続時に割り当てられるWAN側のグローバルIPアドレス、または手動で入力したIPアドレスが表示されます。 ※接続時にグローバルIPアドレスが割り当てられる場合、接続のたびに違うIPアドレスが割り当てられることがあるので、その都度確認して下さい。
サブネットマスク	接続時に割り当てられるサブネットマスク、または手動で入力したサブネットマスクが表示されます。
デフォルトゲート	接続時に割り当てられるゲートウェイの IP アドレス、または手動で入力したゲートウェイの IP アドレスが表示されます。
DNSサーバアドレス	接続時に割り当てられるDNSサーバのIPアドレスが表示されます。
ドメイン名	接続時に割り当てられるドメイン名が表示されます。
DHCPの状態	接続時にWAN側のIPアドレスが割り当てられているときは「取得済み」と表示されます。
リース取得日時	WAN側のIPアドレスが割り当てられた日時が表示されます。
リース取得期限	割り当てられたWAN側のIPアドレスを使用できる期限が表示されます。

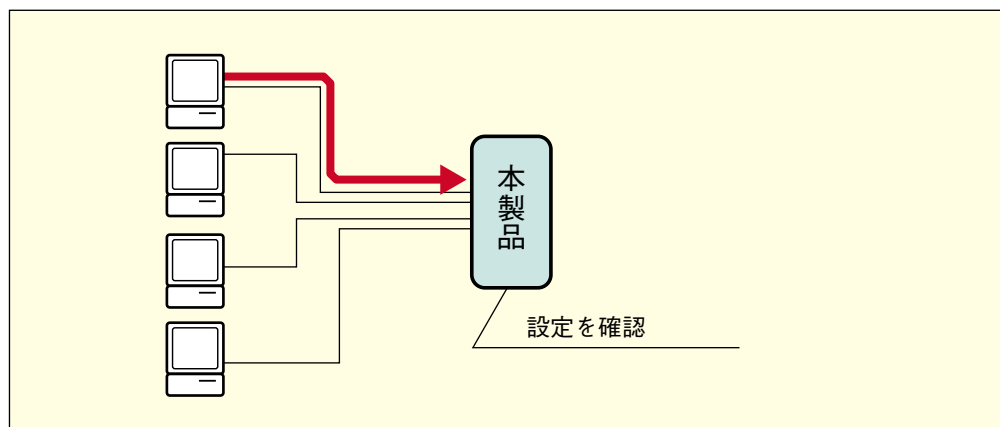
2 本製品のIPアドレスを確認する

本製品のIPアドレスは、［詳細設定］→［ルータ設定］→［LAN］画面で確認できます。

設定ページ

1. ［詳細設定］→［ルータ設定］→［LAN］をクリックします。

   ［ルータ設定（LAN）］画面が表示されます。［本体のIPアドレス/サブネットマスク長］を確認して下さい。

3 設定を確認する

［情報表示（設定）］画面では、本製品のルータ機能に関する設定をまとめて確認できます。

設定ページ

1. ［メンテナンス］の［情報表示］→［設定］をクリックします。

   ［情報表示（設定）］画面が表示されます。

   ※下記の図は、表示例です。

情報表示(設定)　Help

◆現在の設定情報の一覧です。

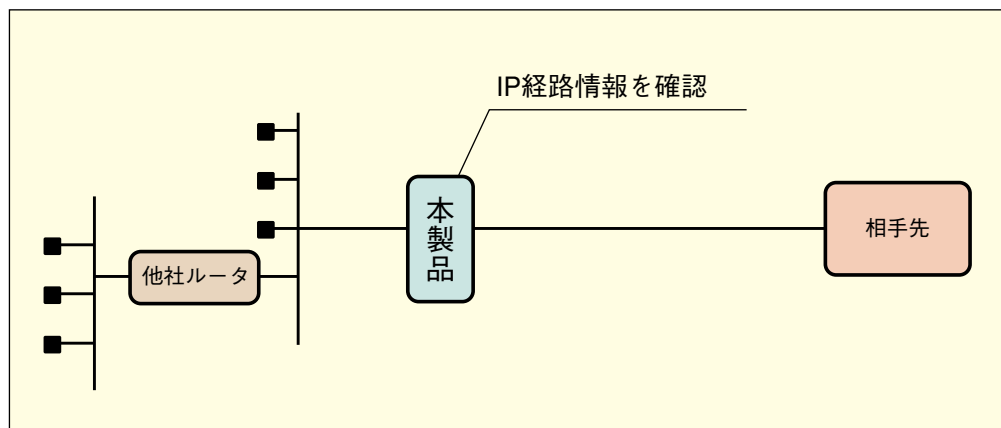
```
# MN8100WAG 1.00 May 31 2004 23:34:57
# MAC Address: 00:80:98:0c:00:02
sys encrypt aee239ecf05c77c1
ip address 192.168.1.1/24
ip dhcp server on
ip dos mode on
ip dos log on
ip filter 59 reject out * 169.254.0.0/16 * * * wanany
ip filter 60 reject dns qtype 6
ip filter 61 restrict out * * tcpfin * * wanany
ip filter 62 restrict out * * tcp_udp * 137-139 wanany
ip filter 63 restrict out * * tcp_udp 137-139 * wanany
ip filter 64 restrict out * * udp 137 domain wanany
logoption type debug off
logoption type info off
logoption type notice on
wireless 0 channel 46
wireless 0 ssid green
wireless 0 auth opensystem
wireless 0 encrypt wep
wireless 0 wep key152 1 74:65:6a:69:6d:61:6b:61:7a:75:6e:6f:72:69:69:69
wireless 0 wep keylength 152
wireless 1 channel 13
wireless 1 ssid green
wireless 1 auth opensystem
wireless 1 encrypt wep
wireless 1 wep key152 1 74:65:6a:69:6d:61:6b:61:7a:75:6e:6f:72:69:69:69
wireless 1 wep keylength 152
wmac filter mode on
wmac filter address 0 00:0b:6b:20:12:c2
```

   購入時の設定から変更した内容が表示されます。

◆［情報表示（設定）］画面でのパスワードの表示

［情報表示（設定）］画面では、パスワードを暗号化したコード（暗号コード）で表示します。暗号コードは、各設定ページで設定を行うごとに更新されます。

4 IP経路を確認する

本製品に登録されているIP経路の情報を確認できます。

設定ページ

1 ［メンテナンス］の［情報表示］→［IP経路］をクリックします。

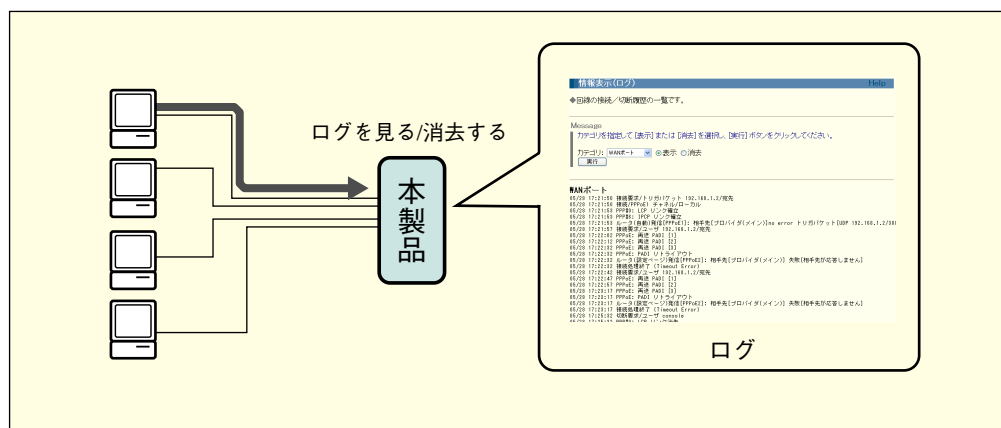
［情報表示（IP経路）］画面が表示されます。

画面には次のような内容が表示されます。

destination	IP経路（ネットワーク番号/サブネットマスク長）
gateway	そのネットワークに到達するための、最寄りのゲートウェイ（ルータ含む）のIPアドレス
mode	IP経路の種別（スタティック、自動接続、RIPなど）
if	IPパケットの入出力ポート番号
metric	そのネットワークに到達するまでに経由するゲートウェイ（ルータを含む）の数（ホップカウント）
ttl	このルーティング情報の有効時間（秒）
remote	相手先番号（スタティック、自動接続のためのIP経路の場合のみ）

5 接続／切断ログを見る・消去する

本製品を使って通信したときの回線接続ごとの記録をまとめて確認できます。記録は、1時間ごとに本製品のフラッシュメモリに保存されるので、電源をOFFにしても記録は失われません。ただし、記録が257件以上になると古い順に自動的に消去されます。また、記録は手動で消去することもできます。

※フラッシュメモリに保存される前に本製品の電源をOFFにすると、直前までの履歴が保存されない場合があります。

設定ページ

1. ［メンテナンス］の［情報表示］→［ログ］をクリックします。

［情報表示（ログ）］画面が表示されます。

保守編

画面には次のような内容が表示されます。

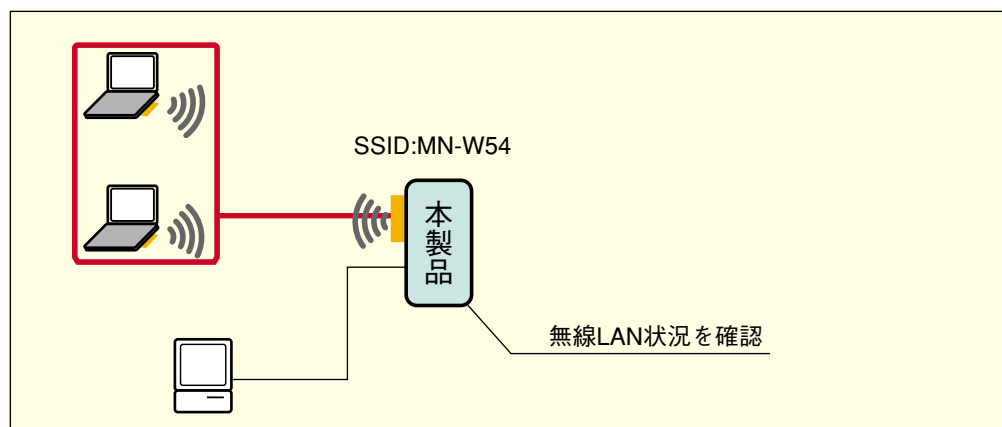
DoS 攻撃防御	DoS 攻撃防御のログを参照できます。
WAN ポート	DHCP クライアント、PPPoE の接続／切断ログを参照できます。
フィルタリング	パケットフィルタリング情報のログを参照できます。
本体制御	本体への設定のログを参照できます。
全て	「DoS 攻撃防御」「WAN ポート」「フィルタリング」「本体制御」のすべてのカテゴリを参照できます。

記録が257件以上になると、古い順に消去されます。

2. 記録を消去する場合は、［消去］ボタンをクリックします。
   とくに必要がない限り、通常は消去しないで下さい。

◆［情報表示（ログ)］画面に正しい日付と時刻を表示させる
正しい日付や時刻を確認するためには、［詳細設定］→［本体設定］の［設定する日付と時刻］に正しい日付や時刻を設定して下さい。

6 無線LAN状況を確認する

設定ページから、本製品の無線LAN機能に関する設定と無線LANに関する通信情報をまとめて確認できます。

設定ページ

1. ［メンテナンス］の［情報表示］→［無線LAN状況］をクリックします。

［情報表示（無線LAN状況）］画面が表示されます。

※下記図は、表示例です。

情報表示（無線LAN状況） Help

◆無線LAN側の機器に関する情報の一覧です。

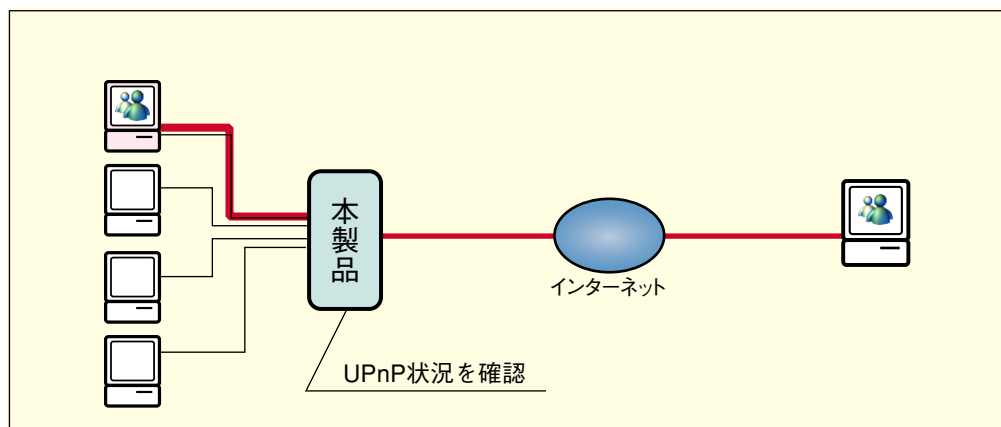
Message

パケット数などの統計情報をリセットするときは[リセット]ボタンをクリックして下さい。

リセット

無線LAN	IEEE802.11a
使用	する
SSID	MN-W54
通信チャネル	34
暗号化	なし
無線LAN端末	なし
送信パケット数	947
送信エラーパケット数	0
受信パケット数	0
受信エラーパケット数	0
無線LAN	IEEE802.11g/b
使用	する
SSID	MN-W54
通信チャネル	11
暗号化	なし
無線LAN端末	なし
送信パケット数	947

7 UPnP状況を確認する

設定ページから、Messengerが本製品に対して要求したポートマッピングの状況を確認できます。

設定ページ

1. ［メンテナンス］の［情報表示］→［UPnP状況］をクリックします。

   ［情報表示（UPnP状況）］画面が表示されます。

   ※下記図は、表示例です。

情報表示(UPnP状況) Help

◆UPnPに関する情報の一覧です。

Message

ポートマッピングテーブルを消去するときは［消去］ボタンをクリックしてください。

消去

UPnP設定

UPnP機能	自動削除設定
ON	自動削除しない

ポートマッピングテーブル

番号	WAN側IP	WAN側ポート	LAN側IP	LAN側ポート	プロトコル	残り時間(秒)
1	133.232.6.97	23456	192.168.1.3	34567	TCP	自動削除しない

◆UPnP状況の削除

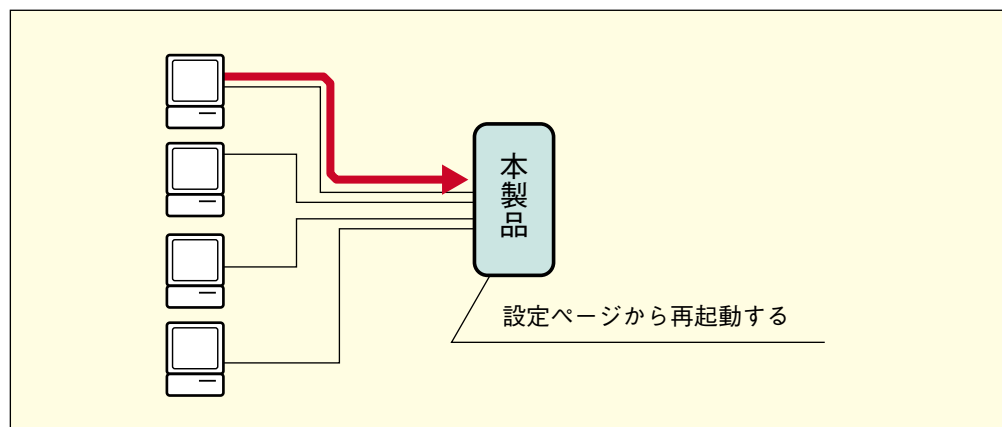
電源を入れ直すと、ポートマッピングの情報は削除されます。

◆UPnP機能を使用しないとき

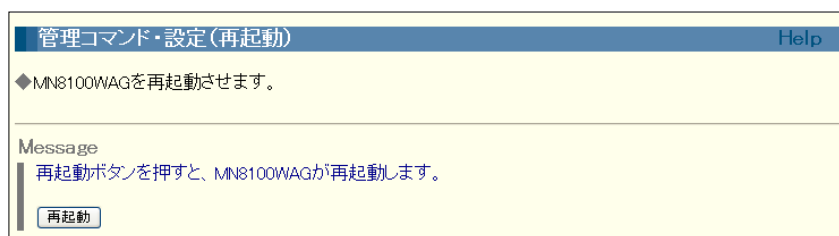
UPnP機能を使わないときは、［詳細設定］→［UPnP設定］画面の［UPnP機能］を［OFF］にします。

保守編

8 本製品を再起動する

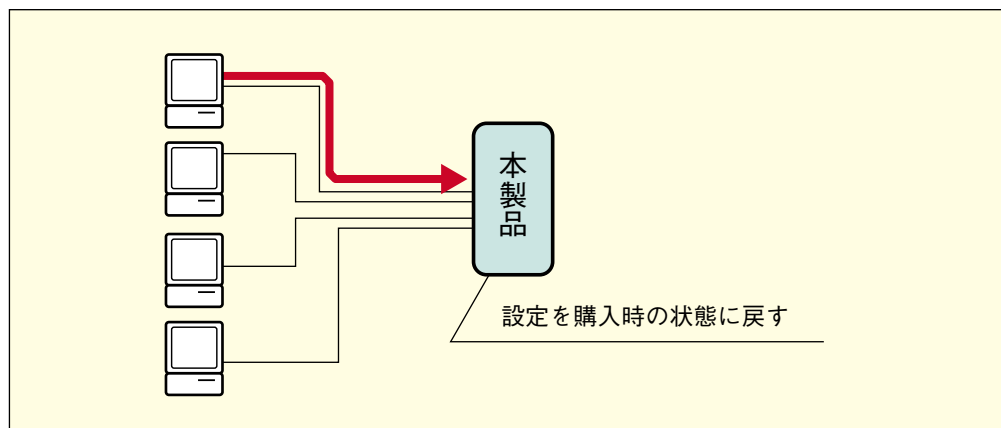
設定ページから本製品を再起動できます。

設定ページ

1. ［メンテナンス］の［管理コマンド・設定］→［再起動］をクリックします。

   ［管理コマンド・設定（再起動）］画面が表示されます。

2. ［再起動］ボタンをクリックします。

   しばらくすると、本製品が再起動します。

9 設定を購入時の状態に戻す

本製品の設定内容を消去して、購入時の設定に戻すことができます。本製品のIPアドレスも、購入時の設定「192.168.1.1」に戻ります。
なお、設定内容を消去する前に、あらかじめ現在の設定内容をファイルに保存しておくことをお勧めします。操作方法については「設定をファイルに保存する／保存した設定を書き込む」〈P.178〉を参照して下さい。

設定ページ

1. ［メンテナンス］の［管理コマンド・設定］→［設定の消去］をクリックします。
   ［管理コマンド・設定（設定の消去）］画面が表示されます。

2. ［消去する設定情報］で、消去する項目を選択します。
   ［すべての設定］を選択すると、すべての内容が購入時の設定に戻ります。
   ※ログは［すべての設定］を選択しても消去されません。それぞれの画面で消去を実行して下さい。

3. ［消去］ボタンをクリックします。

4. 本製品を再起動します。

保守編

10 ユーザIDとパスワードを設定する

本製品にユーザIDとパスワードを設定できます。設定したユーザIDとパスワードを知らなければ、本製品の設定ページを開くことができなくなります。ブロードバンドでインターネットに常時接続する場合は、外部からの侵入を防ぐためにも、必ずこの設定を行って下さい。

※クイック設定で、ブロードバンドで接続の各設定を行う場合にも、ユーザIDとパスワードの設定を行うことができます。

設定ページ

1. ［メンテナンス］の［管理コマンド・設定］→［ユーザ・パスワード変更］をクリックします。

   ［管理コマンド・設定（ユーザ・パスワード変更）］画面が表示されます。

2. 次のように入力します。

ユーザID	12345 ユーザIDを入力します。 ※「no」「clear」は使用できません。
パスワード	pass パスワードを入力します。 ※「no」「clear」「＊（1文字）」「？（1文字）」は使用できません。
パスワード（再入力）	［パスワード］に入力した文字を入力

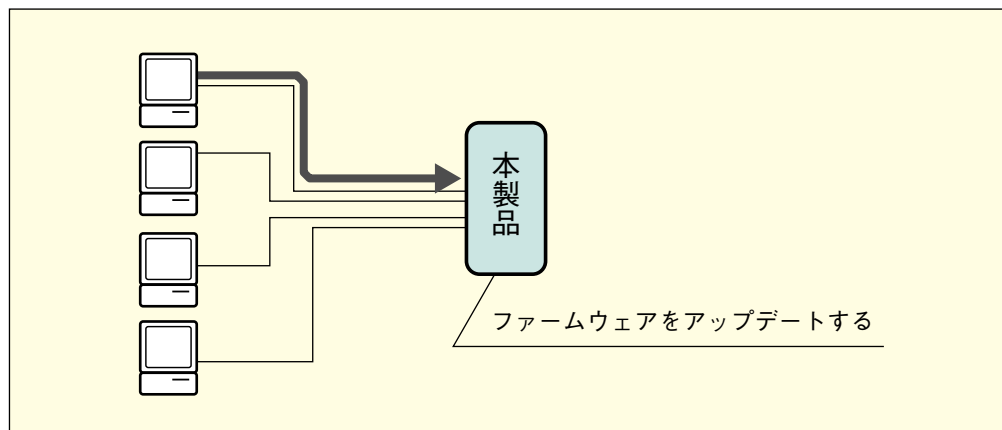
[ユーザ・パスワード変更]	
ユーザID	12345
パスワード	••••
パスワード(再入力)	••••

3. ［設定］ボタンをクリックします。

以降、管理者が設定ページを開くときは［パスワード要求］ダイアログで上記で設定した［ユーザID］と［パスワード］を入力して下さい。また、この設定を行うと、ユーザIDとパスワードを忘れると、設定ページを開くことができません。

◆ユーザIDとパスワードを忘れたとき
ユーザIDとパスワードを忘れて設定ページが開けなくなった場合は、本製品を初期化して購入時の状態に戻す必要があります。この際、設定した内容がすべて消去されるので、ご注意下さい。設定ページが開けないときは、「RESETスイッチの動作について」〈P.182〉を参照して、本製品を購入時の状態に戻して下さい。

11 本製品をアップデートする

本製品の最新のファームウェアは、MN-Informationホームページからダウンロードできます。定期的にMN-Informationホームページにアクセスして最新のファームウェアを入手し、本製品をアップデートして下さい。ダウンロードしたファームウェアのアップデートは、本製品のLANポートにつないだパソコンから行います。

◆あらかじめ設定内容を保存しておくことをお勧めします
安全のため、アップデートを実行する前には設定を保存しておいて下さい。☞「設定をファイルに保存する／保存した設定を書き込む」〈P.178〉

操作

1. WWWブラウザを起動して、MN-Informationホームページにアクセスします。

   MN-InformationホームページのURL
   株式会社 エヌ・ティ・ティ エムイー：http://www.ntt-me.co.jp/mn/

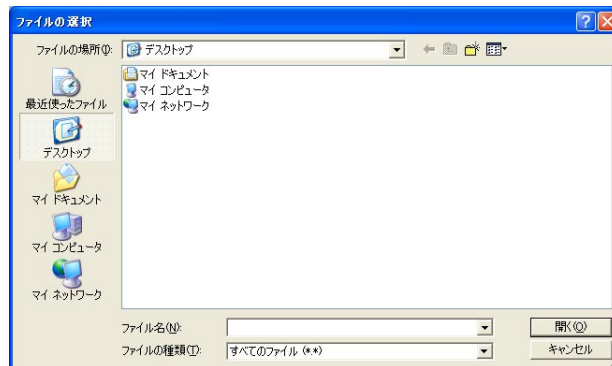
2. アップデート方法のページを表示します。

3. ページの指示に従って、最新のファームウェアファイルをダウンロードします。

4. ファームウェアファイルを、本製品のLANポートにつないだパソコンに保存します。

5. ［メンテナンス］の［管理コマンド・設定］→［ファームウェア更新］をクリックします。

6. ［参照］ボタンをクリックします。

ファームウェアファイルを選択するダイアログが表示されます。

7. ダウンロードしたファームウェアファイルを選択し、［開く］ボタンをクリックします。

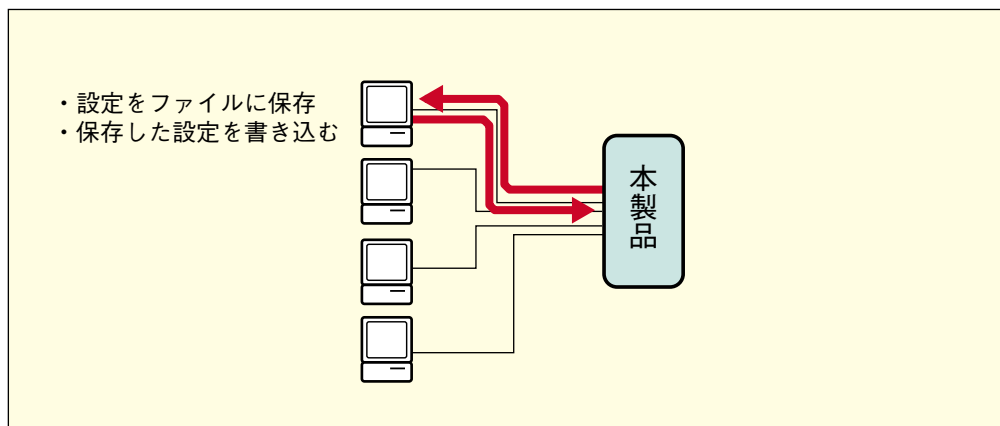
8. ［送信］ボタンをクリックします。

ファームウェアのバージョンアップが開始されます。

ファームウェアの更新には、［送信］ボタン押下後、数秒から10数秒ほどかかります。更新終了のメッセージが表示されるまでお待ち下さい。

保守編

12 設定をファイルに保存する／保存した設定を書き込む

設定ページで設定した内容を、HTML形式のファイルに保存できます。設定をファイルに保存しておくと、別のMN8100WAGに同じ設定をするときや、何らかのトラブルで本製品の設定内容が失われたときなどに利用できます。なお、設定を保存したファイルを「設定ファイル」といいます。

設定を保存するとき

設定ページ

1. ［メンテナンス］の［管理コマンド・設定］→［設定メンテナンス］をクリックします。

   ［管理コマンド・設定（設定メンテナンス）］画面が表示されます。

   画面のテキストボックスには、現在の設定がコマンド一覧で表示されています。
   ※テキストボックス内の文字を、削除したり変更しないで下さい。

2. WWWブラウザの［ファイル］メニューから［名前を付けて保存］や［別名で保存］など、ファイル名を付けて保存するためのコマンドを選択します。

   ファイル名を入力するためのダイアログが表示されます。

3. ファイル名を入力します。

   ［ファイルの種類］で［Webページ、完全（*.htm;html）］を選択します。

   ※保存ファイルのエンコードを選択できるWWWブラウザの場合は、［シフトJIS］を選択して下さい。

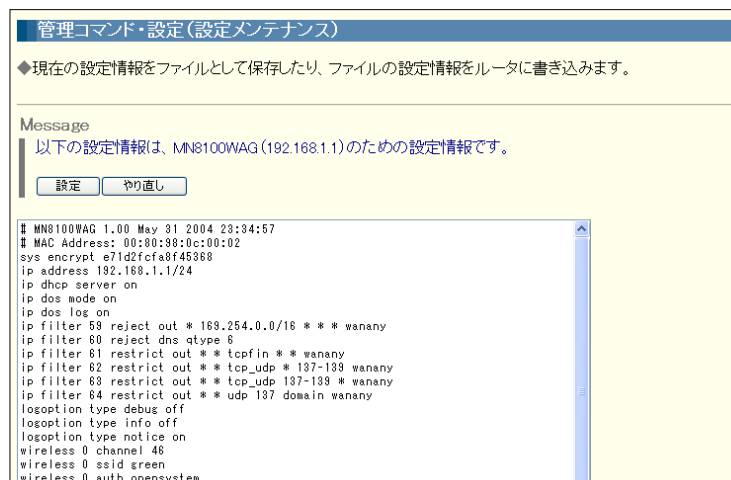
4. 保存を実行します。

   設定ページの内容が、ファイルに保存されます。

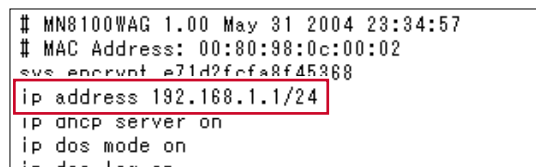
設定内容を本製品に書き込むとき

設定ページ

1. WWWブラウザの［ファイル］メニューから［開く］などのコマンドで設定ファイルを開きます。

   設定ファイルの内容が、WWWブラウザのウィンドウに表示されます。

2. 設定ファイル内の、本製品のIPアドレスを確認します。

   表示されているIPアドレスが、設定を書き込むMN8100WAGのIPアドレスと異なる場合は、表示されているIPアドレスを修正して、設定を書き込むMN8100WAGのIPアドレスに直します。

```
# MN8100WAG 1.00 May 31 2004 23:34:57
# MAC Address: 00:80:98:0c:00:02
sys encrypt e71d2fcfa8f45368
ip address 192.168.1.1/24
ip dhcp server on
ip dos mode on
ip dos log on
```

   ※その他の項目は変更しないで下さい。

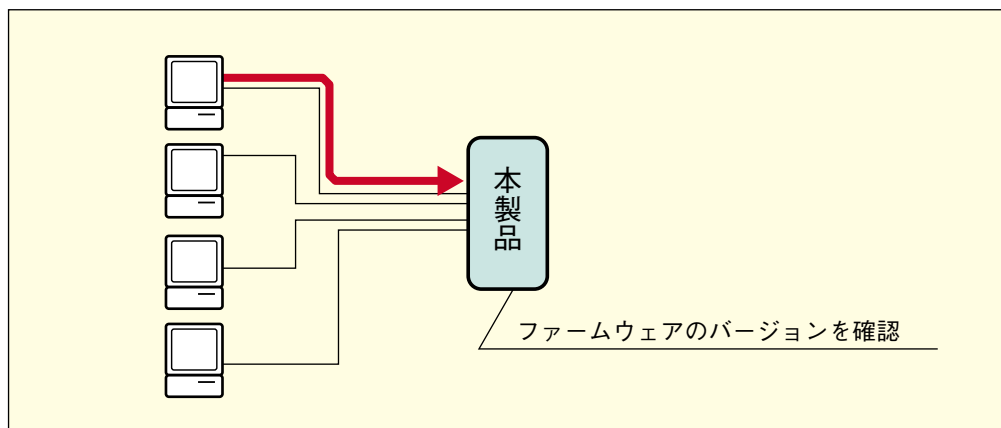
3. ［設定］ボタンをクリックします。

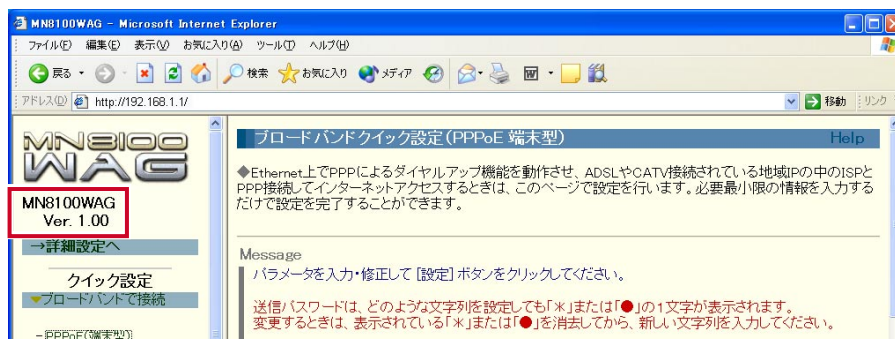
   「設定が終了しました。」というメッセージが表示されます。設定ファイルの内容が書き込まれます。

保守編

［設定ページのアクセス権］でログインユーザIDとログインパスワード、および［PPPoE設定］で送信パスワードを設定した状態で設定ファイルを保存すると、ログインパスワードと送信パスワードは暗号化されてファイルに保存されます。

13 本製品のファームウェアのバージョンを確認する

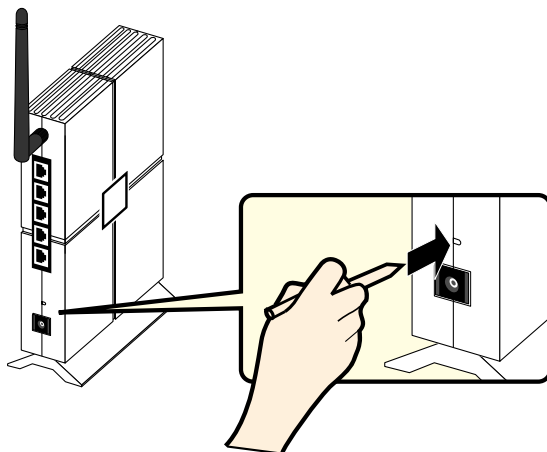
本製品のファームウェアは、不定期にバージョンアップを行っています。お使いのファームウェアのバージョンを確認する方法を解説します。

設定ページ

1. 本製品のLANポートにつないだパソコンから設定ページを開くと、画面左側にファームウェアのバージョンが表示されます。

◆ファームウェアのアップデートについて
本製品の最新のファームウェアは、MN-Informationのホームページで入手できます。
詳しくは、「本製品をアップデートする」〈P.176〉をお読み下さい。

保守編

14 RESETスイッチの動作について

設定ページにアクセスするためのパスワードを失念した場合や、その他の理由で本製品にアクセスできなかった場合は、本製品の設定を初期化できます。初期化を行うと設定内容がすべて失われて、購入時の状態に戻ります。本製品のIPアドレスも、購入時の設定「192.168.1.1」に戻ります。

次の手順を実行すると、本製品は購入時の状態に戻ります。
一度初期化を行うと、設定内容を元に戻すことはできません。ご注意下さい。

操作

1　ACアダプタを接続し、本製品を起動します。

2　起動後、本体背面にあるRESETスイッチを押します。（約10秒）

3　約10秒後、スイッチを離します。
　本製品が購入時の状態に戻ります。

付録

1 困ったときは

ブロードバンドのトラブル

■ブロードバンド接続ができない

→［接続／相手先登録］画面の［送信ユーザID］が正しいか確認して下さい。

→［接続／相手先登録］画面の［送信パスワード］が正しいか確認して下さい。

→ブロードバンド接続には、［PPPoE（端末型）］［PPPoE（LAN型）］［DHCP］［固定IP］の異なる設定方法があります。プロバイダの契約（接続形態）と設定している画面が一致していますか？

→本製品前面のWANのランプを確認して下さい。
点灯していない場合は、ケーブルが外れているか、ケーブルが切断されている場合があります。

→PPPoE/DHCPランプを確認して下さい。
詳細設定で［接続／相手先登録］画面の［PPPoEオプション］にある［PPPoEランプ点灯］で設定を［する］にした場合は、PPPoE/DHCPランプが点灯します。点灯しない場合は［送信ユーザID］［送信パスワード］などの設定を再確認して下さい

→プロバイダの工事は終了していますか？
契約を申し込んでから、工事が完了するまで日数がかかる場合があります。申し込んだプロバイダに確認して下さい。

→クイック設定をしたあと、別のクイック設定をしませんでしたか？
［クイック設定］ページの［PPPoE（端末型）］、［PPPoE（LAN型）］の各画面は、［詳細設定］ページの［接続／相手先登録］画面の各相手先番号と共通です。1つの画面で設定を変更すると、他の画面の設定も同じように変更されます。

■ブロードバンド回線で再接続できない

→ケーブルを抜いたり、正常に切断処理をしないで本製品の電源を切った場合にはしばらく（数分間）再接続できないことがあります。しばらくたってから再接続してみて下さい。

■自動接続できない

→［自動接続相手先］画面で自動接続する相手を変更しませんでしたか？
自動接続したい相手先を選択して下さい。

→［情報表示（IP経路）］画面で自動接続先のルート（［mode］が［auto］と表示されているルート）が正しいか確認して下さい。

→［接続／相手先登録］画面から手動で相手先に接続できるか確認して下さい。

→［ルータ設定（LAN）］画面の［オプション］に登録されているフィルタ、IPアドレス変換テーブルやソース経路情報が正しいかどうか確認して下さい。

→ Windows XP/2000/Meで自動接続できない場合は、次の原因が考えられます。

Windows XP/2000/Meを使用している場合、その仕様により、意図しない自動接続が発生してしまうことがあります。そのため、本製品では、購入時にあらかじめ次のフィルタが登録されています。

ip filter 61 restrict out * * tcpfin * * wanany
ip filter 62 restrict out * * tcp_udp * 137-139 wanany
ip filter 63 restrict out * * tcp_udp 137-139 * wanany
ip filter 64 restrict out * * udp 137 domain wanany

※フィルタ番号は、上記と異なる場合があります。

また、Windows 2000 Serverのドメインに所属するパソコンが、Microsoftネットワークにログオンする場合、Windows 2000 Serverと通信して、ログオン名とパスワードの認証を受けます。その際、Windows 2000 Serverが遠隔地にあるときは、上記のフィルタのために回線を自動接続することができません。
Microsoftネットワークにログオンするときや、共有フォルダへアクセスするときなどに、回線を自動接続したい場合は、［ルータ設定（LAN）］画面の［オプション］に登録されている上記のフィルタを削除して下さい。
ただし、これらのフィルタを削除すると、Windows XP/2000/Meが遠隔地のワークグループまたはドメインに所属する場合、マスタブラウザへ定期的にアクセスするため、回線の自動接続が発生しますので、ご注意下さい。

→ Windows 2000 Serverが自動接続できない場合は、次の原因が考えられます。

Windows 2000 Serverは、電源投入時にパソコンのIPアドレスをDNSサーバに登録する機能があります。そのため、本製品のAutoDNS機能を使用している場合には、パソコンの電源を入れると自動接続を行います。この自動接続を防ぐために、あらかじめ購入時の本製品には、次のフィルタが登録されています。

ip filter 60 reject dns qtype 6

※フィルタ番号は、上記と異なる場合があります。

LAN上のWindows 2000 ServerでIPアドレスをDNSサーバに登録したいときなどに、回線を自動接続したい場合は、［ルータ設定（LAN）］画面の［オプション］に記載されている上記のフィルタを削除して下さい。
ただし、上記のフィルタを削除すると、LAN上にWindows 2000 Serverがある場合、自動接続が発生します。ご注意下さい。

付録

■相手先と通信できない

→ パソコンのTCP/IPの設定が正しいか確認して下さい。

・ パソコンのIPアドレスとサブネットマスクを正しく設定していますか？
・ ゲートウェイを正しく設定していますか？
・ DNSサーバのIPアドレスを正しく設定していますか？

→ 端末型接続する場合、[WAN接続状況] → [PPPoE] 画面の [割り当てIPアドレス] でIPアドレスを取得しているか確認して下さい。

→ フィルタ（[ルータ設定（LAN)] 画面の [オプション] で設定）を正しく登録しているか確認して下さい。

→ 相手先によっては、AutoDNS機能が正常に働かないことがあります。
接続する相手先が設定されている [接続／相手先登録] 画面の [DNSサーバアドレス] に、相手先のDNSサーバのIPアドレスを入力して下さい。

→ ご使用の通信ソフトの設定を確認して下さい。
プロキシサーバを正しく指定していますか？

→ 相手先が他社のルータを使用している場合、スタティックルートの設定が必要なことがあります。☞〈P.71〉

■データ通信中に回線が切断されてしまう

→ [情報表示（ログ)] 画面で「相手先から切断」と表示されているときは、相手先に問い合わせて下さい。

→ [接続／相手先登録] 画面の [自動切断タイマ] を設定していると、設定した時間、回線上で通信がなかったときは自動的に回線が切断されます。自動切断を止めたいときは、[自動切断タイマ] に「0」を設定して下さい。
この場合、接続したら必ず手動で切断して下さい。

特に次の環境で本製品を使用しないように注意して下さい。
・ すでに稼動しているLANに本製品を導入する際、本製品にLANと同じサブネットのIPアドレスを設定しないまま、自動接続を行う設定にしているとき
・ LAN上のパソコンで定期的に回線を接続して通信を行うソフトウェアを起動しているとき

■FTPソフトでファイルの送受信ができない

→次のように、FTPソフトの設定を「PASVモード」に変更して下さい。

・Windows用　NextFTP（Ver.1.91）の場合
[オプション] → [ファイヤーウォール（プロキシ)] タブで [PASVモード] をチェックします。

※FTPによるデータ転送は、通常、サーバ側からクライアント側へアクセスした後にデータ転送を開始する仕組みになっています。しかし、本製品の購入時の設定では、外部からの不正なアクセスを防止するため、WAN側から本製品へのアクセスができないようになっています。そのため、FTPサーバからクライアント側へのアクセスもできません。「PASVモード」とは、この現象を回避するため、クライアント側からサーバ側へアクセスするようにした転送方法です。

■Windows Messenger / MSN Messengerで通信できない

→ 本製品とWindows XP/MeのUPnPの設定を確認して下さい。Messengerを利用するときは、本製品とWindows XP/MeともにUPnP機能をONする必要があります。

・本製品のUPnP設定をONにする

1. ［詳細設定］→［UPnP設定］をクリックし、［UPnP機能］を［ON］にします。

・Windows XPのUPnP設定をONにする

1. ［スタート］メニューの［コントロールパネル］をクリックし、［ネットワーク接続］をクリックします。
［ネットワーク接続］ウィンドウが表示されます。
2. ［詳細設定］メニューから［オプションネットワークコンポーネント］を選択します。
3. コンポーネントの一覧で［ネットワークサービス］をクリックし、［詳細］ボタンをクリックします。
4. ［ネットワークサービス］ダイアログで、［ユニバーサルプラグアンドプレイ］がチェックされているかどうかを確認します。
チェックされていないときは、チェックをつけて［OK］ボタンをクリックします。以降は、Windows XPの画面の指示に従って下さい。

・Windows MeのUPnP設定をONにする

1. ［スタート］メニューの［設定］から、［コントロールパネル］をクリックします。
2. ［アプリケーションの追加と削除］アイコンをダブルクリックして、［Windowsファイル］タブをクリックします。
3. ［コンポーネントの種類］で［通信］をクリックし、［詳細］ボタンをクリックします。
4. ［コンポーネントの種類］ダイアログで、［ユニバーサルプラグアンドプレイ］がチェックされているかどうかを確認します。
チェックされていないときは、チェックをつけて［OK］ボタンをクリックします。以降は、Windows Meの画面の指示に従って下さい。

→ 通信相手の動作環境を確認して下さい。通信相手がUPnP対応のルータを使用していますか？または、プライベートIPアドレスを使用しているプロバイダ経由で接続していませんか？このような場合は、Messengerで通信できません。

→ Messengerでの通信がなくなってから、本製品のUPnPポート自動削除設定で設定した時間が経過したときは、自動的に使用されていたポートが閉じます。ポートが閉じてから再びMessengerを使いたいときは、Messengerをいったん終了してから、起動し直して下さい。Messengerでサインインし直すだけでは正常に動作しませんのでご注意下さい。

その他のトラブル

■相手先の設定が勝手に変わってしまう

→ ［クイック設定］ページの［PPPoE（端末型）］画面、［PPPoE（LAN型）］画面は、［詳細設定］ページの［接続／相手先登録］画面の各相手先番号と共通です。1つの画面で設定を変更すると、他の画面の設定も同じように変更されます。

■パソコンを再起動すると「IPアドレスが使えない」というメッセージが表示される

→ ［ルータ設定（LAN）］画面の［DHCPサーバ機能］をONにしていますか？

→ ［ルータ設定（LAN）］画面の［開始IPアドレス/個数］で、Ethernet上の端末より少ない個数を設定していませんか？

→ DHCPサーバ機能で割り当てるIPアドレスとパソコンの組み合わせを固定していますか？

固定する場合、ホスト情報に登録するパソコンのIPアドレスを、DHCPサーバ機能で割り当てることができる範囲内（［ルータ設定（LAN）］画面の［開始IPアドレス/個数］）で設定して下さい。

■本製品と通信できない／設定ができない

→パソコンのTCP/IPの設定が正しいか確認して下さい。☞「既存のLAN環境で使用する」〈P.98〉

- パソコンのIPアドレスとサブネットマスクは正しく設定していますか？
- パソコンのIPアドレスは、本製品のIPアドレスと同じサブネットワーク番号で設定していますか？
- ゲートウェイは正しく設定されていますか？
- DNSサーバのIPアドレスは正しく設定されていますか？

→ WWWブラウザの［オプション］メニューなどで、「プロキシサーバ（あるいはプロクシ）を使用しない」ように設定して下さい。

- 使用しているWWWブラウザの設定で「必要時にインターネットに接続する」などの項目を選択していませんか？
- 使用しているWWWブラウザの設定で「プロキシサーバー経由で接続する」などの項目を選択していませんか？

→ WWWブラウザのURLを指定する欄に、「http://［本製品のIPアドレス］/」を入力して設定ページを開いてみて下さい。

開くことができない場合は、パソコンでのIPアドレスの設定が正しいか確認して下さい。☞「既存のLAN環境で使用する」〈P.98〉

→ 設定ページで設定するときにエラーが表示されていないか確認して下さい。

→ お使いのパソコンがWindowsの場合は、MS-DOSプロンプト画面などでpingを入力して、パソコンと本製品が正しくIP通信しているかどうか確認して下さい。

→ ルータ機能に関する設定を消去して、最初から設定し直してみて下さい。詳しくは、「設定を購入時の状態に戻す」〈P.173〉を参照して下さい。

→ ファームウェアを再アップデートして下さい。☞「本製品をアップデートする」〈P.176〉

■本製品の設定をファイルとして保存できない

→ 設定ファイルを保存するとき、ファイルを保存するダイアログでファイルの種類を［HTML］や［HTMLソース］などを選択して保存しましたか？

設定ファイルは、HTML形式にして下さい。

■設定ファイルの設定内容を本製品に書き込めない

→［本体設定］画面の［本体の名称］の設定を変更したあとで、パソコンを再起動しましたか？

本製品の名前を変更した場合、本製品の名前で設定ファイルを読み込むためには、パソコンを再起動する必要があります。

→ 設定ファイルが壊れている可能性があります。

■設定したパスワードを忘れてしまった

→ 本体のRESETスイッチを使って、ルータ機能の設定を購入時の状態に戻して下さい。詳しくは、「設定を購入時の状態に戻す」〈P.173〉を参照して下さい。

付録

2 クイック設定で自動的に設定されるフィルタ

クイック設定で、接続の設定を行うと［ルータ設定（LAN）］画面のオプション欄に次のフィルタが自動的に設定されます。
※フィルタ番号は異なる場合があります。

［ブロードバンドで設定］→［PPPoE（端末型）］

下記のフィルタで、「remote 0」のフィルタは「メイン：接続相手先登録#0」を設定すると追加されます。「wanany」のフィルタはクイック設定すると、必ず設定されるフィルタです。なお、サブセッション（接続相手先登録#1～#4）を設定した場合は、「wanany」のフィルタのみ適用されます。

● WAN（Ethernet）側からの不正アクセスを防止するフィルタ

ip filter 57 reject in * 〈本体のIPアドレス〉/32 tcpest * * wanany
ip filter 58 reject in * * tcpest * * wanany

フィルタ#57によって、WAN側から本製品へアクセスすることができなくなります。とくに必要がない限り、削除しないで下さい。
フィルタ#58によって、WAN側からTCPのセッションをオープンすることができなくなります。LAN上のサーバを外部に公開する場合などは、このフィルタを削除するか、WAN側からアクセスできるフィルタ（“pass in”）を登録して下さい。

● WAN（Ethernet）側からの送信元IPアドレスが不正なパケットを破棄するフィルタ

ip filter 45 reject in 10.0.0.0/8 * * remote 0
ip filter 46 reject in 172.16.0.0/12 * * remote 0
ip filter 47 reject in 192.168.0.0/16 * * remote 0
ip filter 48 reject in 10.0.0.0/8 * * remote 1
ip filter 49 reject in 172.16.0.0/12 * * remote 1
ip filter 50 reject in 192.168.0.0/16 * * remote 1

● 送信先IPアドレスの不正なパケットがWAN（Ethernet）側へ送るのを防止するフィルタ

ip filter 51 reject out * 10.0.0.0/8 * remote 0
ip filter 52 reject out * 172.16.0.0/12 * remote 0
ip filter 53 reject out * 192.168.0.0/16 * remote 0
ip filter 54 reject out * 10.0.0.0/8 * remote 1
ip filter 55 reject out * 172.16.0.0/12 * remote 1
ip filter 56 reject out * 192.168.0.0/16 * remote 1
ip filter 59 reject out * 169.254.0.0/16 * wanany

フィルタ#51、#52、#54、#55は本体に設定されているIPアドレスがグローバルIPアドレスの時のみ設定されます。
フィルタが設定されたあとに本体のIPアドレスを変更した場合は、そのIPアドレスにあわせてフィルタを設定し直して下さい。

● LAN上にWindows 2000 Serverがあるときに発生する、「意図しない自動接続」を防止するためのフィルタ（購入時の状態で設定されています。設定をすべて初期化した場合にも自動的に設定されます。）

ip filter 60 reject dns qtype 6

● LAN上にWindows XP/2000/Meがあるときに発生する、「意図しない自動接続」を防止するためのフィルタ（購入時の状態で設定されています。設定をすべて初期化した場合にも自動的に設定されます。）

ip filter 61 restrict out * * tcpfin * * wanany
ip filter 62 restrict out * * tcp_udp * 137-139 wanany
ip filter 63 restrict out * * tcp_udp 137-139 * wanany
ip filter 64 restrict out * * udp 137 domain wanany

このフィルタによりこのままではMicrosoftネットワークを利用して相手先の共有フォルダにアクセスができなくなる場合がありますので、必要に応じて削除して下さい。
"tcpfin"は、TCPセッションの終了（FIN）パケット及びリセット（RST）パケットのみを対象とします。

［ブロードバンドで設定］→［PPPoE（LAN型）］

下記のフィルタで、「remote 0」のフィルタは「メイン：接続相手先登録#0」を設定すると追加されます。「wanany」のフィルタはクイック設定すると、必ず設定されるフィルタです。なお、サブセッション（接続相手先登録#1～#4）を設定した場合は、「wanany」のフィルタのみ適用されます。

● WAN（Ethernet）側からの不正アクセスを防止するフィルタ

ip filter 63 reject in * 〈本体のIPアドレス〉/32 tcpest * * wanany
ip filter 64 reject in * * tcpest * * wanany

フィルタ#63によって、WAN側から本製品へアクセスすることができなくなります。とくに必要がない限り、削除しないで下さい。
フィルタ#64によって、WAN側からTCPのセッションをオープンすることができなくなります。LAN上のサーバを外部に公開する場合などは、このフィルタを削除するか、WAN側からアクセスできるフィルタ（“pass in”）を登録して下さい。

● WAN（Ethernet）側からの送信元IPアドレスが不正なパケットを破棄するフィルタ

ip filter 47 reject in 10.0.0.0/8 * * remote 0
ip filter 48 reject in 172.16.0.0/12 * * remote 0
ip filter 49 reject in 192.168.0.0/16 * * remote 0

● 送信先IPアドレスの不正なパケットがWAN（Ethernet）側へ出るのを防止するフィルタ

ip filter 50 reject out * 10.0.0.0/8 * remote 0
ip filter 51 reject out * 172.16.0.0/12 * remote 0
ip filter 52 reject out * 192.168.0.0/16 * remote 0
ip filter 53 reject out * 169.254.0.0/16 * wanany

フィルタ#50、#51は本体に設定されているIPアドレスがグローバルIPアドレスの時のみ設定されます。
フィルタが設定されたあとに本体のIPアドレスを変更した場合は、そのIPアドレスにあわせてフィルタを設定し直して下さい。

● RIPのDirected-Broadcastに関するフィルタ

ip filter 59 pass in * 〈本体の属するネットワークアドレス〉/32 udp route route remote 0 nolog
ip filter 60 pass in * 〈本体の属するブロードキャストアドレス〉/32 udp route route remote 0 nolog
ip filter 61 reject in * 〈本体の属するネットワークアドレス〉/32 * remote 0
ip filter 62 reject in * 〈本体の属するブロードキャストアドレス〉/32 * remote 0

● LAN上にWindows 2000 Serverがあるときに発生する、「意図しない自動接続」を防止するためのフィルタ（購入時の状態で設定されています。設定をすべて初期化した場合にも自動的に設定されます。）

ip filter 54 reject dns qtype 6

● LAN上にWindows XP/2000/Meがあるときに発生する、「意図しない自動接続」を防止するためのフィルタ（購入時の状態で設定されています。設定をすべて初期化した場合にも自動的に設定されます。）

ip filter 55 restrict out * * tcpfin * * wanany
ip filter 56 restrict out * * tcp_udp * 137-139 wanany
ip filter 57 restrict out * * tcp_udp 137-139 * wanany
ip filter 58 restrict out * * udp 137 domain wanany

このフィルタによりこのままではMicrosoftネットワークを利用して相手先の共有フォルダにアクセスができなくなる場合がありますので、必要に応じて削除して下さい。
"tcpfin"は、TCPセッションの終了（FIN）パケット及びリセット（RST）パケットのみを対象とします。

[ブロードバンドで接続] → [DHCP] / [固定IP]

● WAN（Ethernet）側からの不正アクセスを防止するフィルタ

ip filter 57 reject in * 〈本体のIPアドレス〉/32 tcpest * * wanany
ip filter 58 reject in * * tcpest * * wanany
フィルタ#57によって、WAN側から本製品へアクセスすることができなくなります。とくに必要がない限り、削除しないで下さい。
フィルタ#58によって、WAN側からTCPのセッションをオープンすることができなくなります。LAN上のサーバを外部に公開する場合などは、このフィルタを削除するか、WAN側からアクセスできるフィルタ（“pass in”）を登録して下さい。

● WAN（Ethernet）側からの送信元IPアドレスが不正なパケットを破棄するフィルタ

ip filter 51 reject in 10.0.0.0/8 * * wanether
ip filter 52 reject in 172.16.0.0/12 * * wanether
ip filter 53 reject in 192.168.0.0/16 * * wanether

● 送信先IPアドレスが不正なパケットがWAN（Ethernet）側へ出るのを防止するフィルタ

ip filter 54 reject out * 10.0.0.0/8 * wanether
ip filter 55 reject out * 172.16.0.0/12 * wanether
ip filter 56 reject out * 192.168.0.0/16 * wanether
ip filter 59 reject out * 169.254.0.0/16 * wanany

フィルタ#54、#55は本体に設定されているIPアドレスがグローバルIPアドレスの時のみ設定されます。
本体をリモートアクセスサーバとして使用する場合はこのフィルタを削除するか、または必要に応じてフィルタを追加して下さい。
フィルタが設定されたあとに本体のIPアドレスを変更した場合は、そのIPアドレスにあわせてフィルタを設定しなおして下さい。

● LAN上にWindows 2000 Serverがあるときに発生する、「意図しない自動接続」を防止するためのフィルタ（購入時の状態で設定されています。設定をすべて初期化した場合にも自動的に設定されます。）

ip filter 60 reject dns qtype 6

● LAN上にWindows XP/2000/Meがあるときに発生する、「意図しない自動接続」を防止するためのフィルタ（購入時の状態で設定されています。設定をすべて初期化した場合にも自動的に設定されます。）

ip filter 61 restrict out * * tcpfin * * wanany
ip filter 62 restrict out * * tcp_udp * 137-139 wanany
ip filter 63 restrict out * * tcp_udp 137-139 * wanany
ip filter 64 restrict out * * udp 137 domain wanany

このフィルタによりこのままではMicrosoftネットワークを利用して相手先の共有フォルダにアクセスができなくなる場合がありますので、必要に応じて削除して下さい。
"tcpfin"は、TCPセッションの終了（FIN）パケット及びリセット（RST）パケットのみを対象とします。

3 お問い合わせ先

メンテナンスサービスについて

・ 本製品に含まれるソフトウェアが保存されている媒体に欠陥があった場合、お買い上げの販売代理店または小売店に返却して下さい。無償にて新品と交換いたします。なお、欠陥品送付にともなう送料は、送り主負担とさせていただきます。

・ 本製品に含まれるハードウェアが購入後、1年間に通常のご使用において故障した場合、これを保証します。故障品に保証書を添えて、お買い上げの販売代理店または小売店に返却して下さい。無償にて修理いたします。なお、修理品送付にともなう送料は、送り主負担とさせていただきます。

・ 保証期間でも次のような場合には、有償修理になります。

(1) 保証書のご提示がない場合
(2) 保証書に機器の製造番号、ご購入日、販売店名の記入がない場合、または字句を書き替えられた場合
(3) 接続しているほかの機器に起因して生じた故障、または不当な修理や改造、調整をされた場合
(4) 使用上の誤り、または故意・他意に関わらず、ほかの要因による損傷および故障の場合
(5) 火災、地震、風水害、落雷、そのほかの天災地変、公害や異常電圧による損傷および故障の場合
(6) 購入後の輸送、移動時の落下など、お取り扱いが不適当なため生じた損傷および故障の場合
(7) 購入後の取り付け場所の移動、落下などにより生じた損傷および故障の場合

お問い合わせ先

本製品について技術的なご質問、または製品アップデートに関するご質問は、お買い上げの販売代理店、小売店、またはMNテクニカルセンタまでお問い合わせ下さい。

MNテクニカルセンタ

Tel. 0570-055-128（NTT一般電話、携帯電話用）
Tel. 03-5550-8420（PHSおよびNTT以外の電話用）
Fax. 0570-056-128

9:40～17:50　（土・日・休日・年末年始を除く）

付録

ホームページのご案内

株式会社 エヌ・ティ・ティ エムイーのホームページにて、製品のサポート情報、マニュアル、最新のファームウェア、アプリケーションなどを提供する予定ですので、ご活用下さい。

株式会社 エヌ・ティ・ティ エムイー「MN Information」
http://www.ntt-me.co.jp/mn/

4 用語解説

ADSL（Asymmetric Digital Subscriber Line）

上り方向と下り方向の通信速度が非対称な高速データ通信技術です。すでに一般家庭に普及している電話線を使って、インターネットへの高速で安価な常時接続環境を提供します。

ADSL モデム

ADSL を利用する場合に、サービス加入者側に設置するモデムです。

CHAP（Challenge Handshake Authentication Protocol）

PPP接続で使用されるユーザ認証方法の１つです。最初にPPPサーバがChallenge Valueという乱数をPPPクライアントに送ります。PPPクライアントはその乱数を使ってパスワードを演算し、その結果をPPPサーバに返します。PPPサーバは受け取った値と自分で計算した値とを比較し、同じであれば接続を許可します。
Challenge Valueは認証のたびに変えるため、同じユーザ名とパスワードでも演算の結果は毎回異なります。したがって、たとえ通信回線を盗聴されても、不正利用される可能性は低くなります。ユーザ名とパスワードだけで単純に認証するPAPよりセキュリティの高い方法といえます。

DHCP（Dynamic Host Configuration Protocol）

TCP/IPネットワークにおいて、クライアントがシステムの起動に必要なプログラムをサーバから自動的に取得するプロトコルです。
DHCPサーバは、ネットワークに関連した情報（IPアドレス、デフォルト・ルータのIPアドレス、設定ファイルのファイル名、ドメイン名）などを管理しています。DHCPクライアントが起動すると、DHCPサーバが自動的にIPアドレスを割り振ります。
DHCPクライアントに割り当てるIPアドレスの有効期限を設定できます。有効期限を過ぎると割り当て済みのIPアドレスを再利用することができるので、効率よくIPアドレスを使用することができます。
本製品のDHCPサーバ機能を使う場合、DHCPサーバをサポートしているTCP/IPでは、IPアドレスのほかにデフォルト・ルータのIPアドレスなどが割り当てられます。

DHCPサーバ機能

IPを利用したネットワーク（IPネットワーク）で必要な設定を一元管理し、起動したDHCPクライアントに設定情報を与えるサーバ機能です。

DMZ （DeMilitarized Zone ）

LAN 側のネットワークとインターネットとの間に、ルータを介して設けられる区域のことです。
インターネットにWWWサーバなどを公開することによってLAN 型で接続している端末に、インターネットから不正な接続がされる可能性を減らすために、サーバをこの区域に設定します。

DNS（Domain Name System）

TCP/IPネットワークにおける名前解決サービスのことです。DNS（ドメイン・ネーム・システム）にしたがってドメインネームサーバにコンピュータ名やドメイン名を登録して、ドメインネームサービスを提供しています。ドメインネームサービスを利用すると、「192.168.0.1」などの分かりにくい数字ではなく、分かりやすいドメイン名やホスト名で目的のサイトを指定することができます。

FTP（File Transfer Protocol）

TCP/IPネットワークでファイルを転送するためのプロトコル、またはそのサービスを指します。FTPはおもに、ホストから自分のコンピュータへのファイル転送に使われます。インターネット上に多数存在するFTPサーバから、フリーウェアやシェアウェア、サウンドや画像のデータをダウンロードしたり、自作のプログラムやデータをFTPサーバへアップロードして公開しています。

FTTH（Fiber To The Home）

電話局から各家庭まで光ファイバを引き、高速な通信環境を提供するサービスです。
NTT 東日本、NTT 西日本によって提供されている「B フレッツ」サービスもこれに含まれます。

IEEE 802.11a

IEEE（米国電気電子学会）によって規定された規格で、5GHz 帯の無線で最大54Mbps の伝送を行います。

付録

IEEE 802.11b
IEEE（米国電気電子学会）によって規定された規格で、2.4GHz 帯の無線で最大11Mbps の伝送を行います。

IEEE 802.11g
IEEE（米国電気電子学会）によって規定された規格で、2.4GHz 帯の無線で最大54Mbps の伝送を行います。
IEEE 802.11b の約5 倍の伝送速度をサポートします。

IP（Internet Protocol）
TCP/IPネットワークにおけるネットワーク層プロトコルです。ネットワーク内またはネットワーク間のデータパケット送受信を制御するコネクションレス型プロトコルです。

IPCP（Internet Protocol Control Protocol）
PPPは主に、LCPとNCP（Network Control Protocol）の2種類のプロトコルで構成されています。NCPは、ネットワーク層プロトコルをPPP環境で使用するための制御機能を実現します。NCPはネットワーク層プロトコルごとに規定する必要があり、IP用に規定されているのがIPCPです。クライアントへIPアドレスを割り当てたりします。

IP Masquerade
LAN側で使用している複数のプライベートIPアドレスとWAN側で使用している1つのグローバルIPアドレスを対応付けする機能です。この機能によって、グローバルIPアドレスが1つしか割り当てられない場合でも、LAN側の複数台のパソコンが同時にインターネットを利用できるようになります。

IPsec（Security Architecture for Internet Protocol）
暗号通信のための規格の1つです。IPのパケットを暗号化して送受信するので、TCPやUDPなど上位のプロトコルを利用するさまざまなサービスを保護できます。IPsecは、通信を行う上でのセキュリティを確保するために、「機密性の確保」「完全性の確保」「送信元の確保」「否認の防止」が守れるように設計されています。これによありPPTPよりもセキュリティが強固なVPNを実現できます。

IPフィルタ
→「フィルタ」

L2TP（Layer2 Tunneling Protocol）
L2TPは、Microsoft社が提唱した「PPTP」とCisco Sytems社が開発した「L2F」の2つのプロトコルの仕様をもとに開発された、PPP通信をトンネリングするためのデータリンク層のプロトコルです。L2TPは暗号化機能が実装されていないので、IPsecと組み合わせた利用方法が一般的です。

MACアドレス
ネットワーク上の個々の端末を区別するための物理アドレスです。すべてのEthernetカードには固有のアドレスが割り当てられていて、これを元にデータの送受信が行われます。アドレスはIEEE（アメリカ電気電子学会）によって世界的に管理されています。

MTU（Max Transfer Unit）
TCP/IPのパケットサイズの最大値を決めるパラメータのことです。

PPP（Point to Point Protocol）
遠隔地にある2 点間でパケットを送受信するために設計されたWAN 用のプロトコルで、インターネットに接続するための代表的なプロトコル。パケットにはプロトコルを示すフィールドがあるので、TCP/IP やIP X 、AppleTalk など、複数のプロトコルを同時にサポートできます。

PPPoE（PPP over Ethernet）
PPP フレームを直接Ethernet 上にマッピングして転送するプロトコルです。IETF RFC2516 で規定されています。

PPPoE マルチセッション
1 回線上で、同時に複数のPPPoE 接続を可能にする機能です。

PPTP（Point to Point Tunneling Protocol）
PPPパケットをIPパケットでカプセル化して、IPネットワークに通すことを可能にするプロトコルで、PPPパケットを通すためのトンネル（Tunneling）の役割を果たします。また、カプセル化するIPパケットにユーザIDやパスワードなどの認証用データを格納して送信するので、送信元と送信先でのユーザ認証が実現できます。

SSID（Service Set Identifier）
端末が接続先の無線アクセスポイントを指定するIDです。同じSSID を持つ機器同士のみ接続できます。

UPnP（Universal Plug and Play）
インターネットで標準になっている技術を元にして、家庭内にあるパソコンやAV機器、電話、家電製品などをネットワークにつなぐだけで利用可能にすることを目指した技術です。本製品はこの技術に対応しており、同じくUPnPに対応したアプリケーションソフトである「Windows Messenger」や「MSN Messenger」を利用して、複雑な設定なしにインターネット上での通話を行うことができます。

VPN（Virtual Private Network）
インターネットを利用して論理的なグループを構成し、そのグループ間でセキュリティを保つ仕組みを設けたネットワークのことです。VPN によって、特定のユーザ間を専用回線のように結ぶことができます。

WINS（Windows Internet Name Service）
Windowsのコンピュータ名とIPアドレスを結びつける名前解決サービスの１つです。WINSクライアントは起動するとWINSサーバにコンピュータ名とIPアドレスを登録し、WINSサーバは定期的に各サブネットのコンピュータ名とIPアドレスの情報を交換します。WINSクライアントは、WINSサーバからサブネットをまたがる他のWINSクライアントのコンピュータ名とIPアドレスの情報を取得することができます。

WEP（Wired Equivalent Privacy）
無線LANの国際規格のIEEE802.11できめられている暗号化技術です。アクセスポイントと端末の両方で、同じ文字列からなる「キー（鍵）」を設定しておき、そのキーを使ってデータの暗号化や復号化が行われます。

WWW（World Wide Web）
インターネット上に分散しているファイルやサービスなどの、コンピュータに存在する情報を参照・検索できる仕組みのことです。この仕組みを利用すると、世界中に点在しているテキスト、音、画像などの情報を共有することができます。

WWW ブラウザソフト
ホームページを閲覧したり、WWWサーバを検索したりするためのソフトウェアです。マイクロソフト社の「Internet Explorer」、ネットスケープ・コミュニケーションズ社の「Netscape Navigator」は、代表的な製品です。

アクセスポイント
無線LANカードを装着したパソコンと有線LANの通信を中継したり、無線LANカードを装着したパソコン同士の通信を中継する機器のことです。

サブネット/サブネットマスク
32ビットで構成されるIPアドレスは、クラスに応じてネットワーク番号とホスト番号に分けられます。
ネットワーク番号は、固有のネットワークに割り当てられ、各ホストにはホスト番号を割り当てます。
このとき、サブネットマスクを指定すると、ネットワークの中でさらにサブネットを指定することができ、ネットワーク構築の自由度が上がります。サブネットマスクは、32ビットのうちサブネットとして指定したい部分を１で表し、「11111111.11111111.11111111.00000000」などのように設定しますが、通常10進数で「255.255.255.0」のように表します。

スイッチングハブ
パソコンなどの端末から送られてきたデータをMACアドレスをベースに解析し、送り先の端末だけにデータを送信する機能を搭載しているハブのことです。

スタティックルーティング
ユーザがあらかじめ中継経路（ルーティングテーブル）を固定的に設定する方式のことです。

スタティックルート
ユーザがあらかじめ決めた中継経路のことです。

ステートフル・パケット・インスペクション（SPI）
ファイヤーウォールを通過するパケットのデータを読み取って内容を判断し、動的にポートを開放したり閉鎖したりする機能です。

ステルスモード

インターネット側から送信されるPingコマンド（ポート打診）に応答せず、またICMPエラーやTCPリセットを返さなくなる機能です。外部からの不正侵入のために行われることもある外部からのポートスキャンに反応しないので、インターネット上で本製品の存在を隠すことができます。

セッション

ネットワーク上の2つのホスト間の通信のことです。個々のホストは、同時に複数のセッションを行うことができます。

ダイナミックルーティング

ルータ同士で経路情報やトラフィック情報をやりとりすることによって、中継するルータの数や遅延時間が最小になる最適な経路を自動的に選択して、パケットを転送する方式のことです。

デフォルトルータアドレス

送り先不明のパケットが送られるルータを「デフォルトルータ」といいます。
また、デフォルトルータを示すIPアドレスのことを「デフォルトルータアドレス」といいます。

デフォルトルート

パケットを送信するときに、そのアドレスがルーティングテーブル内に明示的に記載されていないときに使用される、デフォルトルータまでの経路のことです。

ドメイン名

インターネットに接続するコンピュータはIPアドレスと呼ばれる数字を使って識別されていますが、数字よりも簡単に覚えられるように考えられた文字で表現された名前のことです。
ドメイン名は、文字の並びであるラベル、あるいはピリオドで区切られた複数のラベルから構成されます。

例）株式会社 エヌ・ティ・ティ エムイーのドメイン名
ntt-me.co.jp
上記の場合、ntt-me、co、jpの3つのラベルがあり、ドメイン名としてはntt-me.co.jp、co.jp、jpの3つのレベルのドメインから構成されます。

ドメイン名解決要求／解決応答

DNS（ドメインネームシステム）サーバには、ドメイン名と対応するIPアドレスが登録されています。
通信したい相手のIPアドレスがわからない場合、DNSサーバにドメイン名を問い合わせると、そのドメイン名に対応するIPアドレスが通知されます。

ニーモニック

複雑な情報や長い情報を、簡単で覚えやすいものと結びつけるのに使用される単語など、記憶の助けになるものを指します。

パケット

ネットワーク上を流れるデータの単位で、制御信号からなるヘッダと情報データを含むビット列のことです。ヘッダには宛先アドレスや送信元アドレス、データの内容を表わすフラグなどが記録されており、プロトコルや通信方法によって多様です。

ハブ

LANを拡大するためのハードウェアです。ハブには複数のポートがついていて、各ポートにパソコン、ワークステーション、サーバなどを接続できます。ハブにルーティング、ネットワーク管理などの機能が追加され、ネットワークの中心となっているものもあります。LANを構築する場合、10/100BASE-Tケーブルを使用するときは、ハブが必要になります。

光回線終端装置

光ファイバによるインターネットを利用する場合に、サービス加入者側に設置する装置です。

ファームウェア

ハードウェアを動作させるプログラムです。MN Information ホームページからダウンロードできます。

ファイアウォール

内部のネットワークへ、外部から侵入されることを防ぐシステムです。内部のネットワークと外部のネットワークの境界でデータを監視し、不正なアクセスを検出したり遮断したりします。このシステムが組み込まれたコンピュータ自身をさして「ファィアウォール」と呼ぶこともあります。

フィルタ
通過しようとするデータになんらかの処理を施すものです。アドレスを元に、通すパケットと通さないパケットを判別するために使用します。

フィルタリング
通すべきでないデータを遮断することです。
トラフィックの増大を防いだり、不正なアクセスを防いだりします。

ブロードキャスト
同一のネットワーク内のすべてのハードウェアへパケットを送信すること（同報通信）です。

ブロードキャストアドレス
ブロードキャストの際、パケットの送り先に指定するIPアドレスのことです。

ブロードバンド
xDSL、CATV、光ファイバなど、帯域幅が広く転送能力が高い通信方式の総称です。

ホスト
インターネットでは、WWWサーバやメールサーバなどの各種サービスを行うコンピュータをホストとして扱います。

ポート番号
通信を行うアプリケーションとTCPまたはUDPを対応付ける番号のことです。

ホップカウント
パケットが伝送されている間に通ったルータの数を指します。RIPではホップカウントを16に制限しています。

リセット（RST）パケット
このパケットは、再送信などの通常の方法で回復できないエラーが発生した場合や、サーバがシステムダウンした場合に使われます。

5 仕様一覧

ハードウェア

項目		仕様
WANインタフェース		
ポート数		1ポート
コネクタ形状		8ピンモジュラージャック(RJ-45)
物理インタフェース		IEEE802.3/IEEE802.3u
通信速度		10BASE-T:10Mbps/100BASE-TX:100Mbps(AUTO MDI/MDI-X対応)
通信モード		半二重/全二重(自動判別)
LANインタフェース		
ポート数		4ポート
コネクタ形状		8ピンモジュラージャック(RJ-45)
物理インタフェース		IEEE802.3/IEEE802.3u
通信速度		10BASE-T:10Mbps/100BASE-TX:100Mbps(AUTO MDI/MDI-X対応)
通信モード		半二重/全二重(自動判別)
無線LANインタフェース		
準拠規格	国際規格	IEEE802.11a/IEEE802.11g/IEEE802.11b
	国内規格	ARIB STD-T71/ARIB STD-T66
変調方式*	IEEE802.11a	OFDM(直交周波数分割多重)方式
	IEEE802.11g/b	OFDM方式/DSSS(直接スペクトラム拡散)方式
送受信周波数	IEEE802.11a	5.15~5.25GHz
	IEEE802.11g/b	2.4~2.4835GHz
チャネル数	IEEE802.11a	4
	IEEE802.11g/b	13
通信速度	IEEE802.11a/g	54/48/36/24/18/12/9/6Mbps(速度自動切替)
	IEEE802.11b	11/5.5/2/1Mbps(速度自動切替)
最大無線端末数		推奨10台以下
ユーザインタフェース		
状態表示ランプ	POWER(Green)	通電状態表示
	11a(Green)	5GHz帯無線LANの送受信状態表示
	11g(Green)	2.4GHz帯無線LANの送受信状態表示
	PPPoE/DHCP(Green)	PPPoEおよびDHCPの接続状態表示
	WAN(Green)	WANインタフェースの送受信状態表示
	LAN1~4(Green)	LAN1~4インタフェースの送受信状態表示
RESETスイッチ		押しボタンスイッチ
アンテナ		
外部アンテナ		デュアルポールアンテナ(2.4G/5GHz)×1
内部アンテナ		デュアル内蔵アンテナ(2.4G/5GHz)×1
動作環境		
動作温度		5~35℃
保存温度		-10~55℃
動作湿度		5~85%(結露しないこと)
保存湿度		5~85%(結露しないこと)
その他		
電源(ACアダプタ)		AC 100V 50/60Hz 20-30VA、定格出力 DC5V 2.5A
消費電力		9W以下
外形寸法(本体のみ)		約30(W)*×139(D)×173(H)mm(ゴム足、アンテナ含まず) *スタンド部は60(W)mm
質量		約300g(ACアダプタ含まず)
適合規格		特定無線設備技術基準適合認定、電気通信端末機器技術基準適合認定、VCCIクラスB

ソフトウェア

項目		仕様
ルータ機能		
WANインターフェース	PPPoEクライアント	○
	PPPoEマルチセッション	○(最大4セッション同時接続)
	PPPoEセッションキープアライブ	○
	MTU値調整	○(自動調整/手動調整)
	DHCPクライアント	○
	IP固定接続	○
IP Unnumbered		○(複数固定グローバルIPアドレス対応)
DHCPサーバ		253件(固定IP可)
ルーティング対象プロトコル		IP
ルーティングプロトコル		RIP
DNS代理応答(DNSリレー)		○
簡易DNSサーバ		○
VPNパススルー		PPTP、L2TP、IPsec
DMZホスト		○(静的NAT以外のすべてのアクセスを特定ホストに転送)
UPnP		○(最大4ユーザ)
Windows Messenger対応		○
時刻修正		○
セキュリティ	NAT(アドレス変換)	静的32件/動的
	NAPT(IPマスカレード)	静的32件/動的(NATと共用)
	NATセッション数	4096
	IPパケットフィルタ	静的64件
	SPI	○
	ステルスモード	○(WANからのpingに応答しない、ICMPエラーを返さない)
	不正アクセス検出	○
	管理者設定	○(設定ページにアクセスするための管理者ID/パスワード)
無線LAN機能		
IEEE802.11a		○
IEEE802.11g/b		○
Super AG™		○
セキュリティ	SSID	○
	無線LANステルス機能	○(SSIDの隠蔽/ANYプローブ応答禁止/ANY接続拒否)
	WEP	64/128/152bit
	WPA	WPA-PSK(TKIP/AES)
	MACアドレスフィルタリング	○(11a/11g合わせて32件)
管理		
設定	WWWブラウザ(オンラインヘルプ)	○
ログ、状態表示	WWWブラウザ	○

*:OFDM変調は、IEEE802.11a/IEEE802.11g通信時になります。
※本製品は日本国内専用です。日本国外ではご使用になれません。
※本製品を5GHz帯でご使用になる場合は、電波法の定めにより屋外ではご使用になれません。
※Bluetooth製品との通信はできません。

製品お問い合わせ用紙

トラブルなどが発生した場合は、このページをコピーして必要事項をご記入の上、MNテクニカルセンタまでFAXして下さい。

ユーザ情報	
ふりがな 氏名	電話番号 FAX番号
連絡先 〒	

製品情報	
製品名　MN8100WAG	ファームウェアバージョン Ver.
購入日　　年　月　日	製造番号

使用パソコン情報	
メーカ名 [　　]	機種名 [　　]
OS [Windows (Me / 2000 / XP)]	OSバージョン [　　]
本製品を接続しているポート [LAN (内蔵 / 増設)]	

使用ソフトウェア情報	
使用ソフト名 [　　]	使用ソフトバージョン [　　]
使用 INF ファイル名（使用している場合）[　　]	

接続情報
接続先　[NTT 東日本・NTT 西日本 { B フレッツ (　　タイプ)、フレッツ・ADSL }・Yahoo! BB・その他 (　　)・アクセスサーバ・ルータ・他 (　　)]
回線速度 [FTTH ・ ADSL ・ CATV]

ネットワーク情報 [Ether 使用 ・ 不使用]		
IP アドレス [　　]	サブネットマスク [　　]	
ゲートウェイアドレス [　　]	デフォルトルータアドレス [　　]	
プリンタ [なし ・ あり]	メーカ名 [　　]	機種名 [　　]
他ルータ [なし ・ あり]	メーカ名 [　　]	機種名 [　　]

症状

※エラーが出ている場合はエラー番号、メッセージも記入して下さい。
※ LAN ポートからご使用の方は、設定ページの内容を別途添付して下さい。
※接続機器構成図を別途添付して下さい。